Singewald Consultants Group BV
Muzenhof
Stadionweg 138-2
1077 SX Amsterdam
e-mail: singewald@privacy.nl
telefoon: 0297 369767

Bureau RMC
t.a.v.de heer H.Lubbers
per e-mail

Amsterdam, 22 september 2022

Betreft: DPIA: Citytraffic statistische winkel index

Geachte heer Lubbers,

Hierbij stuur ik u de DPIA: Citytraffic statistische winkel index.
Deze is afgesloten op 1 september 2022.

Indien u nog vragen heeft of nadere toelichting wenst, dan verneem ik dat.

Met vriendelijke groeten,

mr Alexander J.J.T. Singewald

bijlage(n) -

DPIA: Citytraffic statistische winkel index

Afgerond 22 september 2022

Mr A.J.J.T. Singewald
singewald@privacy.nl

Inhoudsopgave

DPIA: Citytraffic winkel index

Dit document is de DPIA (privacy impact assessment) de Gegevensbeschermingseffectbeoordeling van product/dienstverlening Citytraffic winkel index van Bureau RMC. Een DPIA vindt zijn oorsprong in de Avg (bescherming persoonsgegevens). Met deze DPIA wil Bureau RMC transparant zijn over haar werkwijze, welke (mitigerende) maatregelen er zijn genomen om de persoonlijke levenssfeer te beschermen, bij het verzamelen, verwerken en het rapporteren aan haar opdrachtgevers. Mocht u vragen hebben dan kunt u altijd contact opnemen met Bureau RMC voor een nadere toelichting.

Amsterdam, september 2022

DPIA (privacy impact assessment) de Gegevensbeschermingseffectbeoordeling

A.1. Beschrijf in het kort wat de nieuwe gegevensverwerking (proces/wijziging/project/initiatief) inhoudt. Waarom wil de organisatie deze verwerking gaan uitvoeren? Wat is de scope van deze DPIA?

Bureau RMC maakt en publiceert op aanvraag en ongevraagd zogeheten Citytraffic statistische winkelindexen, die de drukte in bepaalde winkelgebieden (zones) en tijdblokken weergeeft ten opzichte van elkaar per vooraf bepaalde zones en tijdblokken, niet 24/7 onafgebroken. Deze winkelindexen bestaan uit de combinatie van de uitkomsten van verschillende statistische onderzoeken. Dankzij deze winkelindexen die worden gepubliceerd die geen directe of indirecte persoonsgegevens bevatten zijn afnemers van deze winkelindexen, beter in staat om hun winkels en winkelgebieden te managen. Dat wil zeggen:
Wekelijks inzicht in de trend van groei/afname van passanten in een straat of zone, zorgt ervoor dat klanten de effecten van hun acties en maatregelen statistisch kunnen analyseren door die te vergelijken met een landelijke of lokale trend. Door deze statistische informatie af te zetten tegen statistische informatie uit andere zones, zelfde tijdsblokken kan een marktcijfer, ook wel benchmark worden samengesteld.
Daarnaast gebruikt Bureau RMC, Citytraffic statistische winkelindexen, dezelfde techniek om dit statistische onderzoek uit te voeren in opdracht van een Verwerkingsverantwoordelijke, waarbij bureau RMC Verwerker is.
Deze DPIA is van toepassing op beide situaties, RMC als Verwerkingsverantwoordelijke en RMC als Verwerker.
Deze DPIA is van toepassing op de Citytraffic statistische winkelindexen door RMC gebruikte techniek en kan worden gebruikt om:

1. De groei/afname van het percentage passanten in een bepaalde zone, tijdens bepaalde tijdstippen, vast te leggen; en
2. Met deze vaststelling van groei/afname het effect van getroffen maatregelen te berekenen, zoals wat is het resultaat van het autoluw maken van een bepaalde straat (zone) tijdens bepaalde tijdstippen;

Het is steeds aan de Verwerkingsverantwoordelijke, als die er is, om vast te stellen welke vaststellingen er door RMC worden gedaan, in welke zones en gedurende welke tijden.

A.2. Wie is als proceseigenaar verantwoordelijk voor de privacy compliance van de verwerking? Wie is eindverantwoordelijk voor deze verwerking? Vermeld de namen en functies.

1. Proceseigenaar: Bureau RMC met het product Citytraffic statistische winkelindexen
2. Eindverantwoordelijke: Bureau RMC, of een andere Verwerkingsverantwoordelijke die bureau RMC inschakelt.

A.3. Geef aan van welke categorie(ën) van betrokkenen persoonsgegevens worden verwerkt. Geef daarbij aan wat de relatie is tot de betrokkenen.

Mobiele apparaten gebruiken WiFi probe requests, een verzoek aan nabijgelegen WiFi acces points om informatie op te vragen van het netwerk. In deze probe request worden Media Access Control (MAC) adressen van het apparaat in kwestie meegestuurd. Dit zijn uniek identificeerbare indicatoren.

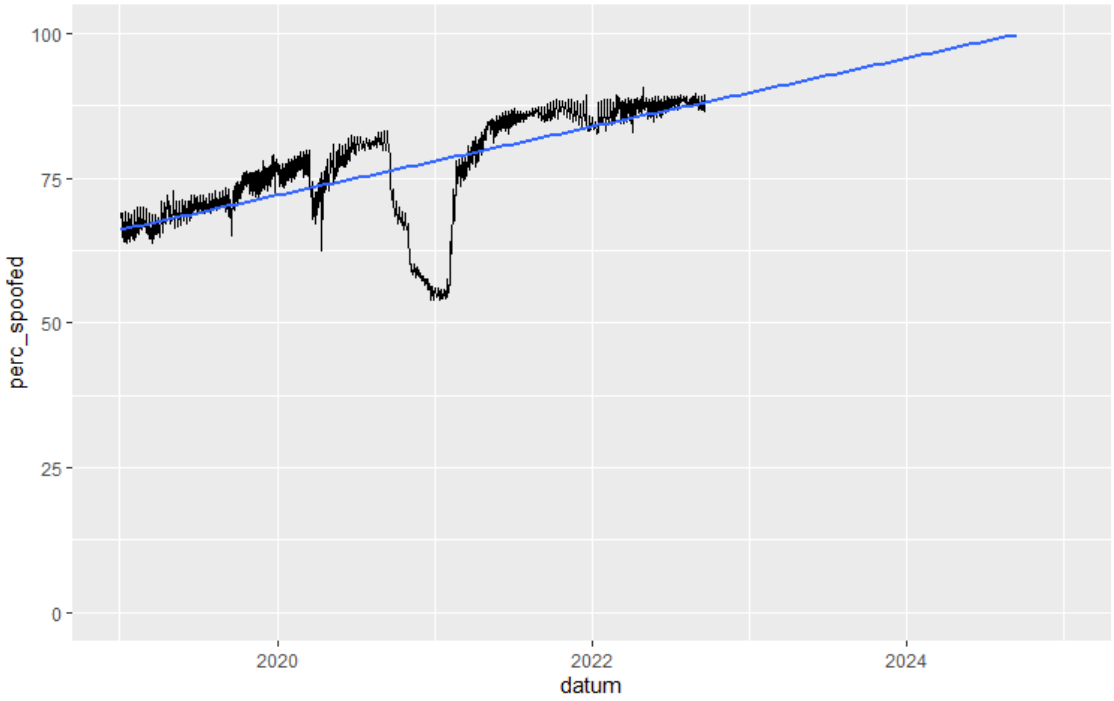
Sinds 2014 hebben de ontwikkelaars van mobiele besturingssystemen, Apple en Google, Mac-adres randomisation toegevoegd.

Randomisation houdt in dat bij probe requests niet meer het daadwerkelijke Mac-adres van een apparaat wordt uitgezonden. In plaats daarvan wordt bij elk probe request een nieuwe willekeurig Mac-adres gegenereerd.

Eerst met IOS 8 door Apple in 2014 en later ook met Android-versie 8 in 2017. Naarmate meer mensen hun randapparaten bijwerken naar de laatste versies of nieuwe randapparaten kopen, kan er op dit moment geconstateerd dat bijna 90% van alle wifi-signalen willekeurig of ‘gerandomised’ is. De verwachting is dat dit uiteindelijk 100% wordt als oude mobiels vervangen worden voor nieuwe modellen.

Zie schema volgende pagina.

Ontwikkeling aandeel randomised tellingen.



Door deze randomisatie is het met (meerdere) meetpunten niet meer mogelijk om bij te houden of bepaalde randapparatuur op verschillende plekken terug te zien is. Voor elk probe request genereert de randapparatuur namelijk een nieuw willekeurig Mac-adres. Daarmee is het niet meer mogelijk om patronen in gedrag van randapparatuur te onderzoeken. Het Mac-adres kan dus niet meer teruggebracht worden tot een direct of indirect persoonsgegeven.

Wat is de werkwijze:

1. De scanners van Bureau RMC verzamelen binnen het bereik van de scanner de probe requests die randapparatuur uitzenden wanneer WiFi aanstaat. Deze data wordt opgeslagen en verwerkt op de servers van Subverwerker PFM.
2. Op de Mac-adressen wordt een hash algoritme toegepast en van het resultaat wordt de tweede helft weggelaten (“afgeknipt”) waardoor dit niet meer terug te brengen is tot het Mac-adres bij meting. Vervolgens wordt de hoeveelheid probe requests geaggregeerd op half uur niveau, welke als basis voor de Citytraffic telmethode wordt gebruikt.
3. Mac-adressen, gehashed en afgeknipt, worden voor de Citytraffic telmethode niet verwerkt door Bureau RMC, maar door subverwerker PFM.

A.4. Geef aan welke categorieën van persoonsgegevens worden verwerkt.

- Indirecte, gehashte persoonsgegevens, per elke probe request dat waargenomen wordt, te weten:

- (gerandomiseerd) Mac-adres van een apparaat,
- tijdstip van aanvang signalering
- tijdstip van einde signalering
- signaalsterkte
- Of de waarneming een gerandomiseerd Mac-adres heeft of niet

A.5. Wat is de herkomst van de persoonsgegevens?

De meeste passanten/bezoekers dragen tegenwoordig randapparatuur bij zich waarop zij wifi aan hebben staan, zoals een smartphone. Aan de hand van de hoeveelheid probe requests dat dit apparaat uitstuurt kan door middel van statistische analyse de afname of groei van drukte worden vastgesteld.

A.6. Aan welke categorieën ontvangers worden de persoonsgegevens verstrekt? Zijn deze als verwerker te kwalificeren?

Er worden geen persoonsgegevens verstrekt bij rapportage, de Citytraffic statistische winkelindexen. In overeenstemming met artikel 89 Avg en overweging 162 Avg worden alleen anonieme gegevens opgenomen in de uitkomsten/rapportages.[1] Citytraffic statistische winkelindexen is een rapportage.
Verwerkingsverantwoordelijke:

1. Bureau RMC, B.2 Building, John M. Keynesplein 12-46, 1066 EP Amsterdam. Bureau RMC maakt gebruik van de diensten van verwerker: PFM Intelligence Group (https://pfm-intelligence.com/); of
2. Andere Verwerkingsverantwoordelijk, die als eigen Verwerkingsverantwoordelijke de techniek wil inzetten. Echter zal deze ook gebruik maken van de diensten van verwerker: PFM Intelligence Group (https://pfm-intelligence.com/)

A.7. Bepaal welke bewaartermijnen voor deze persoonsgegevens van toepassing zijn.

Bureau RMC heeft toegang tot de server van PFM waar tellingen na observatie binnen komen. Tellingen zijn niet direct zichtbaar in deze database, maar hebben altijd een vertraging van 5 minuten tot meer dan een uur. Op de scanner zelf worden Mac-adressen direct bij observatie gehashed en afgeknipt. PFM bewaart deze ingekorte gegevens 24 uur, waarna deze worden verwijderd. Bureau RMC neemt alleen geaggregeerde data over van de server van PFM. Bureau RMC heeft deze afspraken vastgelegd in een zogeheten verwerkersovereenkomst.

[1] Onder statistische doeleinden wordt verstaan het verzamelen en verwerken van persoonsgegevens die nodig zijn voor statistische onderzoeken en voor het produceren van statistische resultaten. Die statistische resultaten kunnen ook voor andere doeleinden worden gebruikt, onder meer voor wetenschappelijke onderzoeksdoeleinden. Het statistische oogmerk betekent dat het resultaat van de verwerking voor statistische doeleinden niet uit persoonsgegevens, maar uit geaggregeerde gegevens bestaat, en dat dit resultaat en de persoonsgegevens niet worden gebruikt als ondersteunend materiaal voor maatregelen of beslissingen die een bepaalde natuurlijke persoon betreffen.

A.8. Beschrijf de doel(en) van verwerking

Voor welke doeleinden de gegevens worden verwerkt wordt bepaald door de Verwerkingsverantwoordelijke. Veel voorkomende doelen voor statistisch onderzoek zijn:

(i) het aantal passanten in een bepaalde straat of zone in een bepaalde periode ten behoeve van statistische tellingen;

(ii) percentage, per dag, per week, per maand of per jaar vergelijkbare uren in drukte weergegeven via vergelijking over dezelfde periode van Citytraffic statistische winkelindexen, immers de daaraan ten grondslag liggende individuele gegevens zijn niet meer beschikbaar, alleen nog als totalen.

A.9. Beschrijf de rechtsgrond(en) van verwerking (meerdere antwoorden mogelijk).

Afhankelijk van wie de Verwerkingsverantwoordelijke is, kunnen verschillende grondslagen van toepassing zijn:
Verwerkingsverantwoordelijke is **particuliere organisatie (zoals Bureau RMC)**, gerechtvaardigd belang organisatie of derde, toestemming
Verwerkingsverantwoordelijke is **overheidsinstantie**: taak van algemeen belang, taak van het openbaar gezag dat aan verweringsverantwoordelijke is opgedragen, wettelijke verplichting die op de verwerkingsverantwoordelijke rust die op grond van, op basis van unierecht of lidstatelijkrecht op de verwerkingsverantwoordelijke van toepassing is.
Zowel voor de particuliere organisatie als de overheidsinstantie zal verder worden getoetst op:

1. Bij het vaststellen van de grondslag zal worden getoetst aan de proportionaliteit (minder ingrijpend) en subsidiariteit (minder vastleggen voor zelfde doel), alsmede aan het belang is van de vragen die worden beantwoord en of het inderdaad vragen zijn die zich statistisch laten beantwoorden.
2. Tot slot zal er worden getoetst aan de genomen beveiligingsmaatregelen en of wordt voldaan aan de eisen met betrekking tot pseudonimiseren en anonimiseren van de persoonsgegevens als beschreven in artikel 89 Avg met betrekking tot statistisch onderzoek en rapportage als in overweging 162 Avg.

B.1. Is een van de drie criteria van artikel 35 lid 3 AVG van toepassing? Zo ja, welke en licht dit toe.

Criterium: Stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.
Deze komt het dichtstbij de dienstverlening van City Traffic Winkelindexen. Alleen wat is stelselmatig en grootschalig? De City Traffic Winkelindexen worden altijd maar ‘tijdelijk’ en binnen een zone (deel van een van een winkelstraat) uitgevoerd en volgen van een persoon is niet mogelijk. Deze DPIA is toch uitgevoerd om transparant te maken hoe het product City Traffic Windelindex tot stand komt. Niet omdat artikel 35 Avg van toepassing zou zijn.
Mac-adressen zijn indirect identificeerbare persoonsgegevens en daarom aan te merken als persoonsgegevens in de zin van de Algemene verordening gegevensbescherming (AVG). Echter zal het tellen steeds beperkt in tijd en in ruimte worden gedaan, dus niet stelselmatig. Dit in combinatie met de mitigerende maatregelen maakt het mogelijk om de City Traffic Winkelindexen als dienstverlening aan te bieden.

B.2. Is/zijn er een of meerdere categorieën van de lijst van de Autoriteit Persoonsgegevens van toepassing? Zo ja, welke en licht dit toe.

- Innovatief gebruik of innovatieve toepassing.
De oudere generatie kent ze nog wel, de man of vrouw met de handmatige personenteller in de hand. Hierop kon het aantal passanten worden geteld, maar terugtellen kon de handmatige personenteller niet. Hierdoor is de man of vrouw met de handmatige personenteller niet langer een alternatief wanneer men het aantal passanten wil vaststellen in een bepaalde zone alsmede de groei of vermindering van het aantal passanten. De informatie is relevant voor het testen van tijdelijke verkeersplannen, bijvoorbeeld om vast te stellen of verkeersmaatregelen bijdragen aan sluipverkeer.
- Inzetten van technologie voor het monitoren en tellen van persoonsgegevens van betrokkenen?
Nee niet monitoren in de zin van 'volgen' en tellen. Het gaat alleen om tellen van aanwezige Wifi-randapparatuur in een bepaalde straat of zone.

B.3. Zijn er twee of meer criteria van de lijst van de WP29|EDPB (European Data Protection Board) van toepassing? Zo ja, welke en licht dit toe.

Locatiegegevens, namelijk de gegevens van een straat of zone waar een wifi-signaal van een gerandomiseerd en niet gerandomiseerd Mac-adres wordt vastgesteld.

B.4. Is er anderszins sprake van een dusdanig hoog privacyrisico dat een DPIA nodig is? Bijvoorbeeld door gebruik van nieuwe technologieën (in combinatie met andere criteria).

Een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen?
Stapsgewijs:

- Er wordt een probe-request waargenomen dat een Mac-adres bevat.
- Op de sensor wordt direct het gemeten Mac-adres gehasht en verkort.
- Het aantal waargenomen probe requests in de zone en tijdsperiode worden vastgelegd in een database voor het maken van de anonieme rapportages en voor kwaliteitscontrole van de data en rapportages voor maximaal 24 uur. De anonieme rapportages worden dan vrijgegeven. De individuele gegevens op basis waarvan de rapportages worden gemaakt worden na 24 uur gewist.

B.5. Volstaat deze Pre-DPIA of is een DPIA verplicht?

Geef op basis van de antwoorden van B.1 tot en met B.4 een eindoordeel of een DPIA verplicht is en licht toe.
Als antwoorden:

C.1. Advies: DPIA uitvoeren, voor transparantie

Het uitvoeren van een DPIA draagt bij aan transparantie.

Beslissing en motivering: uit het bovenstaande volgt dat er bij deze verwerking transparant dient te worden beschreven hoe deze in overeenstemming met de Avg wordt uitgevoerd. De DPIA is hiervoor een goed instrument.

C.2. Beschrijf de aard en de inhoud van de verwerking

Google (Android) en Apple (IOS) hebben recentelijk op hun mobiele randapparatuur het besturingssysteem aangepast waardoor het Wifi protocol anders functioneert: De software in de randapparatuur stuurt continue willekeurige gewijzigde Mac-adressen uit. Dit wordt ook wel aangeduid met niet-gerandomiseerd voor een 'echt' Mac-adres van randapparatuur en gerandomiseerd voor een 'fake' Mac-adres van randapparatuur.

Wat is de werkwijze: De scanners vangen probe request, die een Mac-adres bevatten, op en deze worden geaggregeerd tot half uur niveaus.
Deze verzamelde deels indirecte persoonsgegevens worden door middel van een one way hash en door verkorting teruggebracht tot het aantal randapparatuur. Deze verkorting vindt plaats door zes karakters van de individuele hash af te halen. Hierdoor kan alleen he t aantal randapparatuur worden geteld na verkorting van de hashcode en niet meer het Mac-adres.
Het probe requests wordt als basis genomen om het aantal bezoekers bijvoorbeeld per half uur te schatten. De antitrack&trace software die mobiele fabrikanten als Google en Apple installeren op smartphones, zorgt ervoor dat het originele Mac-adres dat in de telefoon staat vermeld bij de instellingen zelden wordt uitgezonden.
Op basis van de aantal wifi-signalen (gerandomiseerde en niet-gerandomiseerde) bepaalt CityTraffic het aantal passanten per half uur binnen zone. De methode waarop dit automatisch wordt gedaan is als volgt: de ruwe tellingen worden verwerkt tot passantenaantallen per half uur per locatie door de aantallen te verhogen/verlagen met lokale statistische coëfficiënten die het wifi-gebruik symboliseren. Daarna wordt er centraal gevalideerd per week met andere telgegevens, die beschikbaar zijn als stereoscopie-metingen van telsensoren, gps metingen van Google, bezoekersgegevens van andere onderzoeksbureaus (indien voorhanden) en wordt de data aangeboden in rapporten en in dashboards. In deze rapportages worden geen persoonsgegevens aangetroffen.

C.3. Beschrijf de scope van de verwerking.

De klanten van Citytraffic zijn te verdelen in verschillende categorieën:
Er zijn grofweg twee soorten opdrachtgevers: particuliere opdrachtgevers en publieke opdrachtgevers (overheidsinstanties). Scope is om via statistisch onderzoek een zo nauwkeurig antwoord te geven van de passantendrukte binnen een afgebakende fysieke zone, waarbij het antwoord, de rapportage, anoniem is en geen direct of indirecte persoonsgegevens worden verstrekt. Dit wordt wel uitgevoerd in een beperkte zone (winkelgebied, horecagebied, evenemententerrein) en beperkt in tijd (winkelopeningstijden bijvoorbeeld). Het statistisch karakter van de rapportages, gebaseerd op gerandomiseerde en niet-gerandomiseerde Mac-adressen maakt het mogelijk om op basis van anonieme statistische aantallen aan benchmarking te doen.

C.4. Beschrijf de context van de verwerking.

Verwachten betrokkenen deze verwerking en bestaan hierover zorgen?

Betrokkenen verwachten deze verwerking niet en worden hier centraal via websites over geïnformeerd. Er bestaat geen mogelijkheid meer om te opt-outen en het 'tel me niet register' aan te leggen omdat de data niet wordt opgeslagen of kan worden ontdubbeld. Bovendien veranderen de Mac-adressen van smartphones voortdurend waardoor een opt-out register niet effectief zal zijn.

C.5. Beschrijf het doel en het belang van de verwerking.

Doel van de verwerking is de vaststellen door middel van meting en telling van:

(i) statistische informatie teneinde de trend toename/afname in passanten per straat (zone) gedurende halfuurniveau weer te geven.

(ii) statistische informatie teneinde de trend toename/afname in passanten per winkelgebied weer te geven.

subdoel van de verwerking

(iii) de vergelijking van de trend toename/afname in passanten met een benchmark van vergelijkbare steden op basis van anonieme rapportages.

(iv) de vergelijking van de trend toename/afname in passanten met andere perioden op basis van anonieme rapportages.

C.6. Transparantie

Bureau RMC levert standaard informatie aan die kan worden geplaatst op de websites van RMC of opdrachtgevers.

C.7. Rechten betrokkenen

Hoe geef je invulling aan de rechten van betrokkenen en aan privacyvragen en -verzoeken?
De Mac-adressen en gerandomiseerde Mac-adressen die worden vastgesteld worden op de sensor one way-gehasht en verkort en blijven maximaal 24 uur bewaard. Een inzageverzoek naar aangetroffen Mac-adressen heeft geen nut, daar de Mac-adressen onomkeerbaar op de sensor worden gepseudonimiseerd en verkort en deze pseudoniemen na 24 uur worden verwijderd van de server.

C.8. Kennis & awareness

Hoe houd je de privacykennis van medewerkers op het benodigde niveau?
Medewerkers van Bureau RMC dienen bij indiensttreding de Privacyverklaring en het privacy protocol dat periodiek wordt geactualiseerd te bestuderen. Bovendien nemen zij kennis van het huishoudelijk reglement voor security en veiligheidseisen. Alle vaste medewerkers worden ondersteund om hun kennis van AVG te verruimen.

C.9. Verwerkersovereenkomsten

Er is een verwerkersovereenkomst afgesloten met de subverwerkers van Bureau RMC en deze is opvraagbaar. De klanten, die geen Verwerkingsverantwoordelijke zijn, van Bureau RMC hoeven geen verwerkersovereenkomst af te sluiten omdat er geen persoonsgegevens worden geleverd in de rapportages. Klanten krijgen standaard drukte-indexen die wekelijks in een bepaald formaat worden geactualiseerd.

C.10. Autorisaties.

Heb je de autorisaties ingericht op basis van ‘need to know’? (role based access)?
Alleen functionarissen van leverancier PFM voor wie het noodzakelijk is om toegang te hebben voor het plegen van onderhoud aan hardware en software hebben de mogelijkheid om instellingen aan te passen. Analisten van bureau RMC hebben alleen toegang tot de one way-gehashte en verkorte gegevens voor maximaal 24 uur bewaard. De directie heeft autorisatie om haar controlerende taak naar de werking conform specificaties uit te kunnen voeren. Autorisaties zijn dus ingericht op basis van need-to-know voor een bepaalde doeleinden of taak.

C.11. Informatiebeveiliging.

Welke (soorten) beveiligingsmaatregelen heb je getroffen bij deze verwerking? Welke specifieke beveiligingsnormen gelden er voor dit proces? Wordt daaraan voldaan?
Bureau RMC en (Sub)Verwerker hebben passende technische en organisatorische beveiligingsmaatregelen genomen, ter bescherming tegen verlies en misbruik van Mac-adressen, oneway gehashte en verkorte gegevens en die gegevens die onder RMC’s zeggenschap vallen. Bovendien vindt alle communicatie, zoals tussen de sensoren en backoffice servers, de toegang van partners tot de beschikbare passantengegevens en het onderhoud van systemen, plaats via versleutelde verbindingen.
Bureau RMC en haar (Sub)Verwerker hebben onder meer de volgende technische en organisatorische maatregelen getroffen tegen:

a. Openbaarmaking van niet-openbare informatie:
Het expres of onbedoeld openbaar maken (lekken) of wissen van niet-openbare informatie, met inbegrip van privacygevoelige informatie.

b. Vermissing of diefstal van bedrijfsmiddelen:
Diefstal of het kwijtraken van randapparatuur die door Verwerkingsverantwoordelijke of Verwerker worden beheerd, zoals mobiele telefoon, tablet, laptop, toegangspasje of token.

c. Besmetting met schadelijke software (ransomware/malware/virus):
Een besmetting van een werkstation of ander bedrijfsmiddel met schadelijke software, ook wel malware. Hieronder worden ook virussen, randsom en cryptoware verstaan.

d. Aanval op de digitale infrastructuur:
Een doelgerichte aanval op websites die worden gebruikt voor statistisch onderzoek, (web)applicaties of servers met het doel niet-openbare informatie te verkrijgen of de digitale infrastructuur te ontregelen.

e. Storing in hardware door stroomuitval, brand of water:
Een brand- of wateroverlast (lekkage) in ruimten waar zich vitale ICT voorzieningen bevinden die leidt tot een verstoring van dienstverlening.

f. Het opslaan van verzamelde persoonsgegevens op randapparatuur:
Persoonsgegevens opgeslagen op randapparatuur zullen telkens worden gewist per statistisch onderzoek uiterlijk op het moment dat het betreffende onderzoek is afgerond.

g. Het trainen van functionarissen bij interne en externe onderzoeksorganisaties:
Tijdens de trainingen komen de bovenstaande en specifieke onderzoeksorganisatie-eigen technische en organisatorische aspecten aan de orde.
Ook is Bureau RMC lid van brancheverenigingen MOA en onderschrijft ze de zelfregulering die als onderdeel van Fair Data Policy door MOA is opgesteld.

C.12. Datalekkenbeleid.

Beschik je over datalekkenbeleid, een effectieve procedure en een datalekkenregister?
Indien Verwerker bij het verwerken van persoonsgegevens kennis krijgt van een beveiligingsincident, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens, dan zal Verwerker onverwijld, edoch binnen 24 uur na ontdekking, de Verwerkingsverantwoordelijke daar van op de hoogte brengen, terwijl Verwerker in de tussentijd alle mogelijke technische en organisatorische maatregelen neemt om het beveiligingsincident te stoppen, te voorkomen en/of te herstellen. Verwerker verstrekt bij de melding informatie omtrent de aard van de inbreuk, de aard van de gelekte persoonsgegevens, de technische beschermingsmaatregelen en overige relevante feiten en omstandigheden die van belang zijn om te bepalen of de toezichthouder en/of de betrokkene geïnformeerd dienen te worden.

C.13. Kwaliteit.

Bureau RMC beschikt over procedures om de kwaliteit van de gegevens te waarborgen?
Bureau RMC heeft technische en organisatorische maatregelen getroffen om de kwaliteit te waarborgen. Organisatorisch is het van belang om met de resultaten te benchmarken waardoor significante afwijkingen vroegtijdig kunnen worden vastgesteld. Technisch wordt er regelmatig getest of de ‘installatie’ nog goed werkt.

C.14. Afstemming met betrokkenen.

Heb je bij het uitvoeren van de DPIA de betrokkenen om hun mening gevraagd over de verwerking, en zo ja, op welke wijze wordt deze meegenomen in de DPIA?
De volgende deskundigen zijn geconsulteerd door de directie:

- Bart Jaspers, onafhankelijk ICT specialist werkzaam bij SquareNext
- FG-ers van gemeente Den Haag, Spijkenisse, Dordrecht, Maassluis, Alkmaar, Castricum
- Wim van Slooten, directeur MOA
- Victor Hartman, data-analist bij bureau RMC

D.1. Rechtmatigheid. Beoordeel aanvullend op wat hierboven al is uitgewerkt de rechtmatigheid van de verwerking.

Er is sprake van een verwerking in overeenstemming met de Avg, waarbij steeds een juiste grondslag dient te worden gekozen.

D.2. Noodzaak. Zijn alle verwerkingen noodzakelijk voor het bereiken van het doel?

Bureau RMC dient deze tellingen op beperkte basis uit te voeren om haar klanten te bedienen die op haar beurt (management)informatie nodig hebben voor de optimale exploitatie van hun winkels en winkelgebieden en heeft daarbij een bedrijfseconomisch belang. Het tellen van passanten/bezoekers en het maken van een statistische analyse is daarvoor een gebruikelijke bedrijfsactiviteit. Winkelgebieden wensen informatie over drukte tijdens winkelopeningstijden, horecagebieden wensen meer inzicht in de avond en nacht. Hiermee wordt procentueel de verdeling van een groep vastgesteld in de zone ((deel van) winkelgebied). Deze verwerking is dus noodzakelijk om dat doel te bereiken.

D.3. Dataminimalisatie en doelbinding. Zijn alle persoonsgegevens strikt noodzakelijk voor het bereiken van het doel? Wordt aan de eis van doelbinding voldaan?

Ja, de persoonsgegevens die worden verwerkt zijn noodzakelijk om en telling te doen van het aantal passanten. De persoonsgegevens die in opdracht van Bureau RMC worden verwerkt, worden alleen ten behoeve van de managementinformatie van haar klanten gebruikt.
Voorzover doelbinding in deze vraag wordt bedoeld als 'verenigbaar gebruik', wordt opgemerkt dat artikel 5 lid 1 onder b Avg beschrijft dat het gebruik van persoonsgegevens voor statistisch onderzoek nimmer als onverenigbaar met de oorspronkelijke doeleinden kan worden beschouwd. Uiteraard dient er wel sprake te zijn van een grondslag op basis waarvan de persoonsgegevens worden verwerkt.

D.4. Proportionaliteit. Staat de inbreuk op de persoonlijke levenssfeer in evenredige verhouding tot de verwerkingsdoelen?

Bureau RMC heeft een gerechtvaardigd belang om aan de hand van CityTraffic passantentellingen uit te voeren. Mede door de genomen beveiligingsmaatregelen en een minimum aan vast te leggen data, wordt er voldaan aan proportionaliteit. Daarnaast heeft RMC als jarenlange aanbieder van statistische winkelindexen, die de drukte in winkelgebieden weergeeft ten opzichte van elkaar per vooraf bepaalde zones en tijdblokken. Er worden alleen statistische gegevens verzameld die relevant zijn voor de vragen. De terughoudendheid bij het verwerken van persoonsgegevens, het toepassen van one-way hash en verkorting van de reeks en dit in combinatie met de door randapparatuur zelf uitsturen van randomised en niet-randomised Mac-adressen, zonder dat het kenbaar is wat voor Mac-adres het betreft, het leveren van anonieme rapportages en het informeren van de burgers. De genomen voorzorgmaatregelen afwegende tegen de belangen van de consument leidt er in het geval particuliere sector dat de grondslag het eigen gerechtvaardigd belang of van derde is.
In de overheidssector kan men niet terugvallen op de grondslag van gerechtvaardigd belang. Als de afweging zoals hierboven wordt gemaakt zal de overheid moeten terugvallen op artikel 6 lid 1 aanhef onder e. In de bijlage treft u een brief aan van Minister S. Dekker, 3 juni 2020 aan de VNG inzake de grondslag wifi tellen door gemeenten en grondslag voor gegevensverwerking.

D.5. Subsidiariteit. Is er geen andere, voor betrokkene minder belastende manier om hetzelfde doel te bereiken?

De inzet van andere telmethoden waarbij geen persoonsgegevens worden verwerkt om de drukte in binnensteden te tellen, stuiten op onoverkomelijke bezwaren waardoor de methode met de inzet van wifi sterk de voorkeur heeft. Enerzijds omdat het alle gerandomiseerde en niet-gerandomiseerde Mac-adressen in direct via een oneway hash en verkorting van de getal reeks onomkeerbaar geanonimiseerd worden, waardoor er geen reële kans bestaat dat deze aldus bewerkte gegevens herleidbaar, identificeerbaar of koppelbaar zijn, maar anderzijds omdat de uitvoering van de andere teltechnieken op te veel beperkingen stuit. Zie eerder over de handteller die meer alleen zijn eigen zichtlijnen kan gebruiken om het aantal aanwezigen vast te stellen.
Infrarood: is een onbetrouwbare meting voor gebieden waar mensen eenvoudig kunnen stilstaan en kan zelden overdwars in een winkelstraat worden geïnstalleerd. Deze methode is mogelijk interessant voor gesloten winkelcentra maar ook daar wordt deze technologie tegenwoordig aangepast naar stereoscopie of andere sensoren.

Radar: levert een onbetrouwbare meting op tijdens drukke momenten. Geeft een goed beeld op rustige momenten, maar hierdoor niet geschikt voor winkelgebieden.
Stereoscopie: levert een zeer betrouwbare meting, maar dient aan de buitenzijde van een pand of paal te worden bevestigd op een hoogte van minimaal 5 meter waardoor de kansen om dit te realiseren minimaal zijn. Bovendien wegen de kosten van een complete installatie niet altijd op tot het doel van het onderzoek.
Viewer: deze innovatie bestaat pas enkele jaren en heeft een, nog te onderzoeken, betrouwbare telling mogelijk gemaakt door real time te onderzoeken van live beeld met een fotodatabase. Een op het eerste inzicht betrouwbare en AVG veilige methode maar kostbaar en moeilijker te installeren dan een wifi-sensor. In de database wordt de vervoersmodaliteit gecontroleerd en zo kan er een verschil worden gemaakt tussen, voetgangers, fietsers, auto's en bussen.
GPS: apparaten waarbij de locatiegegevens tijdens gebruik op 'aan' staan, worden door Google tegenwoordig aangeboden, tijdens de pandemie. Normaal gesproken is deze informatie niet beschikbaar op een zakelijk niveau. De meting betreft een diffuus omschreven gebied en kan om die reden niet worden gebruikt om precies in winkelgebieden te tellen.

E.1. Geïdentificeerde risico's

Beschrijf en bepaal de (bruto-)risico's voor betrokkenen H/M/L (hoog/middel/laag).
Voor City Traffic winkel index, statistisch onderzoek, worden onder deze PIA de mogelijke volgende risico's onderkend:

1. Identificeren van personen
2. Volgen van personen
3. Volgen van personen in verschillende zones
4. Mac-adres zichtbaar in rapportage
5. Verwerker

Via benchmark worden de volgende onjuiste werkingen gesignaleerd. Deze verwerkingen zullen worden gestopt, de software en hardware zal opnieuw worden gekalibreerd, ter plaatse of op afstand door PFM, het kan dan gaan om:

1. Periodiek doormeten van netwerk
2. Onjuist werkende tijdklok, overschrijding van bewaartermijnen
3. Onjuiste anonimisatie, indien hash niet werkt
4. Verwijderen van informatiemateriaal (maandelijkse inspectie van zones)

E.2. Welke beheersmaatregelen worden er getroffen om de risico's te mitigeren? Risico's staan hierboven

Beoordeel welke technische, organisatorische en juridische maatregelen er kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt en wat het verwachte restrisico is na het uitvoeren van de maatregel. Neem deze beheersmaatregelen op in de kolom 'beheersmaatregelen' van de DPIA. Indien de maatregel het risico niet volledig afgedekt, motiveer dan waarom het restrisico acceptabel is en neem deze motivatie op in het risico-acceptatiedocument.
Benoem per onderkend risico:
Welke beheersmaatregelen kunnen er worden getroffen? Wat is het effect op het bruto-risico? Wat is het restrisico (netto-risico)? Zijn de te nemen maatregelen geaccordeerd om verder te implementeren? Zijn deze al geïmplementeerd?

Algemeen:

Via benchmark worden de volgende onjuiste werkingen gesignaleerd. Deze verwerkingen zullen worden gestopt, de software en hardware zal opnieuw worden gekalibreerd, ter plaatse of op afstand door PFM, het kan dan gaan om:

1. Periodiek doormeten van netwerk
2. Onjuist werkende tijdklok, overschrijding van bewaartermijnen
3. Onjuiste anonimisatie, indien hash niet werkt
4. Herstel van verwijderd informatiemateriaal (maandelijkse inspectie van zones)

Risico nr. 1: identificeren van persoon

Te treffen beheersmaatregelen:

- gerandomiseerde of niet-gerandomiseerde Mac-adressen uitgegeven door de fabrikant van toestel of operating system wordt verwerkt. Dit maakt het volgen van een bepaalde randapparatuur niet mogelijk, tenzij er maar in de zone één randapparatuur aanwezig is, rekening houdend met meettijden en kennis hebben hoe vaak een randapparatuur een Mac-adres uitstuurt;
- realtime Mac-adres, wordt one-way gehasht, en daarna verkort (deel wordt afgeknipt);
- rapportage voor statistisch onderzoek is anoniem (Niet herleidbaar, niet deduceerbaar en niet koppelbaar, conform overweging 162 Avg).

H/M/L/geen: laag risico
Maatregelen akkoord: Ja
Maatregel al geïmplementeerd: Ja
Overige maatregelen/werkzaamheden
• Privacyverklaring verbeteren/aanvullen
• Passanten informeren over sensor gebruik, data retentie en verwerking
• Geldige grondslag verzorgen
• Verwerkersovereenkomst afsluiten
• IBV beleid uitwerken en implementeren
Is voorafgaande raadpleging AP nodig: niet noodzakelijk

Risico nr. 2: volgen van persoon

Te treffen beheersmaatregelen:

- gerandomiseerde of niet-gerandomiseerde Mac-adressen uitgegeven door de fabrikant van toestel of operating system wordt verwerkt, maakt het volgen van een bepaalde randapparatuur niet mogelijk, tenzij er maar in de zone één randapparatuur aanwezig is, rekening houden met keuze meettijden en kennis hebben hoe vaak een randapparatuur een Mac-adres uitstuurt;
- realtime Mac-adres, wordt one-way gehasht, en daarna verkort (deel wordt afgeknipt);
- rapportage voor statistisch onderzoek is anoniem (Niet herleidbaar, niet deduceerbaar en niet koppelbaar, conform overweging 162 Avg).

H/M/L/geen: laag risico

Maatregelen akkoord: Ja
Maatregel al geïmplementeerd: Ja
Overige maatregelen/werkzaamheden
• Privacyverklaring verbeteren/aanvullen
• Passanten informeren over sensor gebruik, data retentie en verwerking
• Geldige grondslag verzorgen
• Verwerkersovereenkomst afsluiten
• IBV beleid uitwerken en implementeren
Is voorafgaande raadpleging AP nodig: niet noodzakelijk

Risico nr. 3.: Volgen van personen in verschillende zones

Te treffen beheersmaatregelen:

- gerandomiseerde of niet gerandomiseerde Mac-adressen uitgegeven door de fabrikant van toestel of operating system wordt verwerkt, maakt het volgen van een bepaalde randapparatuur niet mogelijk, tenzij er maar in de zone één randapparatuur aanwezig is, rekening houden met keuze 'meettijden' en kennis hebben hoe vaak een randapparatuur een Mac-adres uitstuurt;
- realtime Mac-adres, wordt one-way gehasht, en daarna verkort (deel wordt afgeknipt);
- rapportage voor statistisch onderzoek is anoniem (Niet herleidbaar, niet deduceerbaar en niet koppelbaar, conform overweging 162 Avg).

H/M/L/geen: laag risico
Maatregelen akkoord: Ja
Maatregel al geïmplementeerd: Ja
Overige maatregelen/werkzaamheden
• Privacyverklaring verbeteren/aanvullen
• Passanten informeren over sensor gebruik, data retentie en verwerking
• Geldige grondslag verzorgen
• Verwerkersovereenkomst afsluiten
• IBV beleid uitwerken en implementeren
Is voorafgaande raadpleging AP nodig: niet noodzakelijk

Risico nr. 4.: Ingeschakelde (Sub-)Verwerker

Te treffen beheersmaatregelen:

- Compliance onderzoek door RMC bij Verwerker op basis van artikel 28 Avg;
- Geheimhoudingsverklaring;
- Schriftelijke verwerkersovereenkomst cq subverwerkersovereenkomst;

H/M/L/geen: Medium risk
Maatregelen akkoord: Ja
Maatregel al geïmplementeerd: per opdracht wordt de verwerkers of subverwerkersovereenkomst afgesloten.

Is voorafgaande raadpleging AP nodig?
Is voorafgaande raadpleging AP nodig: niet noodzakelijk

F. Algemeen afrondend

De genomen mitigerende maatregelen zijn voldoende. De gevallen als in artikel 35 lid 3 Avg doen zich hier niet volledig voor (augustus 2022). Ook zijn er voldoende mitigerende maatregelen ten aanzien van verwerkingen die door de Autoriteit persoonsgegevens als zodanig zijn gekwalificeerd, zie Staatscourant nr. 64418, 27 november 2019.

Bepaal en omschrijf aan de hand van de resterende risico's of de verwerking mag worden gestart of dat een voorafgaande raadpleging bij de AP nodig is.
Technisch kan wel worden gestart, afhankelijk van de Verwerkingsverantwoordelijke dient de juiste grondslag uit artikel Avg te worden gekozen en de verwerkersovereenkomst en/of subverwerkersovereenkomst dient tot stand de komen.
De meeste risico's zijn te mitigeren door alle bovenstaande maatregelen te treffen.

Uitvoering DPIA

Augustus 2022, was getekend:
mr A.J.J.T. Singewald (uitvoering PIA)

H. Lubbers (directie)

Bijlage, brief minister Dekker 3 juni 2020