Gemeente Amsterdam

Retouradres: Postbus 94652, 1090 GR Amsterdam

Gemeente Amsterdam
Commissie Persoonsgegevens

Aan de Directeur Verkeer & Openbare Ruimte,
mevrouw 5.1, 2, e .1, 2, e
C.C.: Stedelijk directeur Ruimte & Economie, mw. C. Apeldoorn
CIO, de heer J. Flippo
Manager IV Ruimte & Economie, de heer 5.1 5.1, 2, e
Privacy coördinator Ruimte & Economie, mevrouw 5.1, 2, e 5.1, 2, e

Datum	25 juli 2017
Ons kenmerk	U 17054
Behandeld door	Mw. 5.1, 2, e
Doorkiesnummer	5.1, 2, e
Faxnummer	nvt
E-mail	5.1, 2, e @amsterdam.nl
Bijlage	1
Onderwerp	Advies Commissie Persoonsgegevens Amsterdam over Fietsparkeren

Geachte mevrouw 5.1, 2, e en heer 5.1, 2, e,

Op de vergadering van de Commissie Persoonsgegevens Amsterdam (CPA) van 6 juli 2017 waren namens u aanwezig: de heer 5.1, 5.1, 2, e (adviseur Enigma), de heer 5.1, 2, e 5.1, 2, e (gemeente Amsterdam) en mevrouw 5.1 5.1, 2, e (privacy coördinator Cluster Ruimte & Economie).

Bij het agendapunt "Fietsparkeren" is het volgende besproken.

De CPA dankt u voor de heldere presentatie voor de gegevensverwerking ten behoeve van de pilot voor Fietsparkeren.

De CPA adviseert om in de informatie aan Amsterdamse burgers te benadrukken dat door het inchecken met een pas of chipkaart uitsluitend het identificatienummer voor het fietsparkeren wordt vastgelegd en dat dit nummer niet is gekoppeld aan klantgegevens, zodat het parkeergedrag niet te volgen is voor derde partijen.

De CPA verneemt graag of de encryptie van de met de banken uitgewisselde gegevens zodanig is dat deze onomkeerbaar zijn versleuteld zodat banken onmogelijk kunnen achterhalen of en waar er met een bankpas is ingecheckt.

De CPA vraagt om op de hoogte gesteld te worden van de uitkomst van dit onderzoek en ook van de uitkomsten van de pilot Fietsparkeren.

Bij een definitieve keuze voor een werkwijze, adviseert de CPA om gebruik te maken van de risicoanalysemethodiek die de gemeente Amsterdam hanteert, om privacy- en beveiligingsrisico's in kaart te brengen en te documenteren, waaronder een risicoanalyse van de beveiliging en een privacy impact assessment.

Voor het verslag van hetgeen over het agendapunt is besproken, verwijs ik kortheidshalve naar de bijlage bij deze brief.

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 besloten vergadering op donderdag 6 juli 2017

5. Fietsparkeren (Ruimte & Economie)
De heren5.1, 2, e en5.1, 2, e geven een presentatie over de sinds maart lopende proef met digitaal management in de fietsparkeergarages RAI en Paradiso. Om de overlast van geparkeerde fietsen te beteugelen, legt Amsterdam fietsparkeergarages aan bij stations van de Noord/Zuidlijn en op het Leidseplein. In totaal moeten die plaats gaan bieden aan 6000 fietsen. De eerste 24 uur is het parkeren gratis. Daarna moet men gaan betalen. Er moet dus een vorm van registratie en afrekening plaatsvinden. Er wordt nu nog gewerkt met papieren bonnetjes maar men wil komen tot een laagdrempelig, klantvriendelijk geautomatiseerd systeem. In de proef worden drie verschillende toegangspoorten getest. Voor de registratie heeft men verschillende mogelijkheden. Dat kan met een bankpas, met de OV-chipkaart of met een speciale in het wiel gemonteerde fietstag voor abonnementhouders. Er wordt via afspraken met het SHPV (servicehuis parkeer- en verblijfsrechten) aansluiting gezocht bij de systemen voor straatparkeren (Parkmobile en dergelijke). Betaling kan voor dagparkeerders met een bankpas, abonnementhouders betalen per iDeal of via hun straatparkeerprovider. Contant betalen is niet mogelijk. Bij de toegang met een bankpas wordt ten behoeve van het PMS (parkeermanagementsysteem) een uniek token gegenereerd die niet herleidbaar is naar het bankrekeningnummer. Alleen die unieke token en de tijdstippen van aankomst en vertrek worden dan in het PMS vastgelegd. Van de incidentele parkeerder die met een OV-chip binnenkomt, worden het chipkaartnummer en de tijdstippen geregistreerd.
Fietsparkeerders met een abonnement kunnen naar binnen met een OV-chipkaart als ze dat bij het aangaan van hun abonnement hebben aangegeven. Van deze klanten wordt het vrij uitleesbare UID van de chipkaart vastgelegd in het PMS. Van abonnementhouders met een fietstag in hun wiel is de elektronisch uitleesbare ID vastgelegd in het PMS en bij de provider. Het is een voor Nederland uniek experiment en alle partijen zijn bereid eraan mee te werken. De voorwaarden worden in de stalling bekend gemaakt en in de abonnementsvoorwaarden moet de klant toestemming geven voor de koppeling via TLS aan zijn OV-chipkaart of via de provider bij een fietstag. Met het GVB is een bewerkersovereenkomst rond de OV-chipkaart. Voor dit systeem maakt het niet uit of het gaat om een persoonlijke of anonieme chipkaart, alleen de UID van de kaart zelf is van belang. De kaart is ook niet gekoppeld aan de fiets; net als nu bij het bonnetjessysteem kan iemand met een andere fiets naar buiten gaan, mits hij een kaart gebruikt waarmee is ingecheckt.
De benodigde gegevens worden opgehaald bij de incheckpoortjes en zuilen en dan doorgestuurd naar de cloud. Die is in beheer van Pass/Vitoz waarmee een bewerkersovereenkomst is afgesloten. Deze beheerder kan de gegevens inzien, maar is gebonden aan die overeenkomst. Met de data kan men niet meer doen dan bekijken hoe vaak een bepaald entreemiddel gebruikt is. Gegevens over herkomst of iets dergelijks zitten er niet in. TLS is de eigenaar van OV-chipkaarten en daarom is de toestemming van TLS nodig voor het gebruik. Maar de database van het PMS wordt niet gedeeld met TLS. Daar is de klant geen toestemming voor gevraagd en dat is juridisch dus uitgesloten, als het technisch al mogelijk zou zijn. Het is niet bekend of TLS iets weet over de abonnementhouder. Die heeft immers een relatie met de NS, niet met TLS.

Bij het gebruik van de bankpas in dit systeem is op geen enkele manier een relatie te leggen met financiële gegevens, bankrekeningnummers of persoonlijke gegevens. Bij de entree wordt alleen dat unieke nummer aangemaakt ter verwerking in het systeem. In de automaten zit meteen een versleuteling. Op verzoek van de banken zit er wel een waarschuwingssysteem in dat net als bij pinautomaten gestolen passen weigert te accepteren. In de samenwerkingsovereenkomst met de banken is vastgelegd dat dit systeem geen privacygevoelige informatie uit de bankpassen kan halen. Dit gebruik van dè bankpas heeft geen enkele relatie met het saldo of een betaling. Het gaat puur om de registratie van de parkeertijd.
De SHPV krijgt alleen een koppelvlak. De NAW-gegevens blijven bij de provider, maar via het koppelvlak wordt automatisch gecontroleerd of bij het OV-chipkaartnummer een abonnement bij enige provider is afgesloten. Als dat het geval is, volgt een ping en als dat niet het geval is moet de kaarthouder ter plekke met een bankpas betalen.
De gemeente blijft eindverantwoordelijk voor de goede en veilige verwerking van de gegevens.
De praktijk wijst uit dat 90% van de parkeerders binnen 24 uur weer met de fiets de stalling verlaat. De proef verloopt goed en de klanten zijn positief. Het systeem werkt erg intuïtief en sluit goed aan bij bestaande, bekende systemen. Het gaat er nu vooral om de technische kant te testen en de reacties op het gebruik van de bankpas. De proef moet verbeterpunten opleveren voor de volgende aanbesteding. Fietsen van abonnementhouders met een fietstag zijn wellicht in de toekomst wel te achterhalen. Die zou men dan bijvoorbeeld kunnen waarschuwen als een fiets erg lang in de stalling blijft staan, maar alle andere fietsen blijven echt anoniem en niet tot personen herleidbaar.

De CPA adviseert in de communicatie te benadrukken dat door het inchecken met een pas of chipkaart geen persoonlijke gegevens worden vastgelegd zodat door derden niet het parkeergedrag te volgen is. Dit mede indachtig de processen die destijds gevoerd zijn rond het kentekenparkeren en alle gevoelens rond privacy bij Amsterdammers. Dit systeem kan niet bij de persoonlijke bankgegevens komen, maar de CPA wil weten of alles in de hash wel zodanig versleuteld is dat een bank omgekeerd onmogelijk kan achterhalen of en waar er met een bankpas is ingecheckt. De CPA vraagt op de hoogte gesteld te worden van de uitkomst van dat onderzoek.