FG-advies

Aan: Gemeente Hilversum
Van: de functionaris gegevensbescherming
Betreft: de druktemeter

Adviesvraag

Gemeente Hilversum heeft de FG om advies gevraagd over de druktemeter: hoe privacyvriendelijk is die?

Mijn antwoord: de druktemeter waarin de gemeente momenteel voorziet, is zeer privacyvriendelijk.

Dit komt door het privacybeschermende ontwerp van de druktemeter en de instellingen. Naar AVG-normering zijn privacyrisico's volledig uitgesloten.

Dit althans zolang het college de privacybeschermende eigenschappen (waar)borgt volgens de raamafspraken over proceseigenaren en rekenschap in het bestuurlijk privacybeleid.

Utrecht, 17 september 2020

Sergej Katus

Mr. S.H. Katus
Partner bij Privacy Management Partners

Toelichting

1 Over druktemeters

De hier bedoelde druktemeter is een ICT-oplossing om in een afgebakend gebied te kunnen detecteren of zich hierbinnen veel mensen bevinden. Bij het overschrijden van bepaalde drempelwaarden worden drukte-indicaties afgegeven zoals 'normaal', 'druk', 'zeer druk' of 'groen', 'oranje', 'rood'

In het kader van de coronabestrijding stellen druktemeters in staat om personen te waarschuwen tegen verhoogde besmettingsrisico's.

Tegelijkertijd kan er bestuurlijke informatie aan worden ontleend. Bij teveel drukte zou bijvoorbeeld kunnen worden besloten om de toegang tot een gebied te beperken ter bescherming van de openbare orde en veiligheid (publieke gezondheid). Druktemeters kunnen daarnaast ook informatie verschaffen over piek- en daluren in winkelgebieden – wat in economisch opzicht nuttig kan zijn.

2 De privacyrisico's van druktemeters

Of een druktemeter een privacyrisico inhoudt, is een tweede. Hierover kunnen in redelijkheid geen uitspraken worden gedaan zonder de werking ervan te begrijpen. Zelfs wanneer gebruik wordt gemaakt van technieken zoals het opvangen van wifi-signalen, zegt dat nog niets. In die zin zijn berichten over privacyschendingen door 'wifi-tracking' niet noodzakelijk terecht.

Volgens de Algemene Verordening Gegevensbescherming mag pas van een risico worden gesproken wanneer uit een AVG-risicobeoordeling blijkt dat het voldoende aannemelijk is dat iemand door gebrekkige gegevensverwerking over hem/haar, schade lijdt (fysiek, geestelijk, sociaal, of economisch).

Cruciaal is vraag in hoeverre een gegevensverwerking – in dit geval de druktemeter – naar AVG-maatstaven risicovol is.

De wetgever heeft dat omgedraaid, door in de AVG aan de hand van basisprincipes en voorschriften (privacywaarborgen) de norm te stellen voor wat *niet* risicovol is.

Dat punt is bereikt wanneer de gemeente heeft voorzien in een passende mix van maatregelen voor de bescherming van personen bij de verwerking van persoonsgegevens. Dat lijkt een technische kwestie, maar is vooral een bestuurlijke/organisatorische verantwoordelijkheid ('control & accountability').[1]

Naleving van de AVG houdt in dat die privacybeschermende maatregelen daadwerkelijk worden genomen, zodat de risico's zijn gereduceerd. Op de AVG-risicoschaal die de gemeente hanteert, kan de mate van risicoreductie worden aangegeven aan de hand van de scoring van het netto risico (het risico dat resteert na het nemen van passende beschermingsmaatregelen). Hoe dichter bij het nulpunt van de AVG-risicoschaal hoe completer de privacybescherming. Bij volledige risicoreductie is het privacyrisico '0'.

[1] Artikelen 1 en 24-25 AVG.

3 Anonimiteit

De AVG bevat als voorbeeld van privacybeschermende maatregelen 'pseudonimisering' (werken met aliassen). De mate van pseudonimisering kan variëren tussen gemakkelijk herleidbaar naar een bepaalde persoon (gemakkelijk identificeerbaar) tot extreem moeilijk. Het BSN is een goed voorbeeld van een voor gemeenten gemakkelijk herleidbaar pseudoniem: laat alle gegevens over naam, adres en woonplaats weg en de gemeente is nog steeds prima in staat om iemand te identificeren.

Hoe moeilijker die herleidbaarheid, hoe meer tegelijkertijd ook mag worden gesproken van anonimiteit. In het dagelijks spraakgebruik hebben we het daarom meestal over anonimiseren. Er zijn ICT-oplossingen voorhanden om anonimiteit technisch 'in te bakken'.

Bij de meest vergaande anonimisering vindt er volledige en onomkeerbare ontkoppeling plaats tussen de gegevens en de persoon op wie die gegevens betrekking hebben. Gegevens die op een dergelijke manier zijn ontkoppeld, brengen naar hun aard geen enkel privacyrisico meer met zich mee (risicoscore 'o'). Het zijn geen *persoons*gegevens meer maar enkel anonieme 'data' zoals meetgegevens over wegverkeer, lawaai, besmettingen of drukte.

Bij anonieme data stelt de AVG geen verplichtingen meer. Personen kunnen aan dit soort gegevens ook geen AVG-rechten meer ontlenen, behalve de waarborg dat de eindverantwoordelijke blijft bewaken dat er door verandering van omstandigheden niet alsnog privacyrisico's ontstaan.

Hou er rekening mee dat herleidbaarheid geen risico op zich is. Herleidbaarheid houdt enkel in dat een gegevensverwerking in meer of mindere mate impact heeft op een individu (profijt of nadeel) en binnen het beschermingsgebied van de AVG valt.

Belangrijk is ook dat géén anonimisering of lichte anonimisering onder de AVG wel passend kan zijn en sterke anonimisering niet. Wat passend is, is volledig afhankelijk van de context en overige beschermingsmaatregelen waarin wordt voorzien.

De AVG biedt de eindverantwoordelijke – bij de druktemeter is dat het college – ruimte voor het maken van eigen keuzes. Sterke anonimiteit is niet vereist maar kan wel logisch zijn.

4 Beoordeling Hilversumse druktemeter

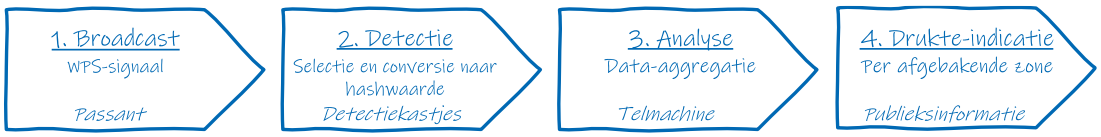
Wat de Hilversumse druktemeter betreft, kiest het college voor een oplossing waarbinnen anonimiteit ICT-matig wordt gegarandeerd. Dit blijkt uit navraag bij de gemeenteorganisatie en de leverancier. Op een schaal van weinig tot volledige anonimiteit, scoort de druktemeter 'volledig'.

Nadere inspectie is een optie maar de uitleg van de gemeente en de leverancier is tot nu toe overtuigend genoeg. Het bestuurlijk privacybeleid bevat bovendien raamafspraken over regievoering, met inbegrip van documentatie van de technische specificaties.

Om de intrinsiek hoge privacybescherming van de druktemeter te waarborgen, is het zaak om die afspraken in de praktijk te brengen bij verdere invoering van de druktemeter. Hierbij dient er vooral op te worden gelet dat de druktemeter doet wat is beloofd op het gebied van anonimiteit.

5 Privacy by design

De anonimiteit die de druktemeter waarborgt, wordt gerealiseerd in drie stappen. Er zit geen tijdsverschil tussen 1 en stap 2 (stap 1 en 2 is gelijktijdig). Het tijdsverschil tussen stap 2 en 3 is te verwaarlozen (milliseconden). Stap 4 is de volledig geanonimiseerde verstrekking van drukte-informatie door de gemeente.



Stap 1 – De 'kastjes' die de gemeente in de openbare ruimte installeert, detecteren dat er mobiele telefoons of vergelijkbare apparaten in de buurt zijn door hun wifi-signalen op te vangen. Waar wifi-signalen zijn, zijn mensen – is de redenering. De wifi-signalen verspreidt iedereen zelf en kunnen met eenvoudige hulpmiddelen ook door iedereen worden opgepikt.

De detectiekastjes letten uitsluitend op het publieke 'WPS-signaal' dat mobiele wifi-apparaten uitzenden zodat andere wifi-apparaten hen herkennen om verbinding te kunnen maken. De detectiekastjes zijn technisch niet in staat om het inhoudelijk wifi-gebruik te zien zoals browsen op internet, e-mailen of Snapchatten.

De informatie in het WPS-signaal zegt weliswaar *iets* over een persoon (kennelijke aanwezigheid), maar zegt niets over iemands identiteit, tenzij iemand zijn of haar naam heeft meegegeven aan het WPS-signaal (bijvoorbeeld 'iPhone Mieke').

De detectiekastjes slaan echter geen acht op dat soort informatie. Automatisch selecteren ze enkel de knipsels uit het WPS-signaal die nodig zijn voor druktemeting.[2]

Stap 2 – Die knipsels converteren de detectiekastjes onmiddellijk en onomkeerbaar naar een bepaalde waarde met behulp van hashing-techniek. Bijvoorbeeld de waarde 698H73365. Die waarde is absoluut onherleidbaar, dus volledig anoniem. De hashwaarde laat zich ook niet meer terugrekenen naar de knipsels. Op het moment dat de hashwaarde is gegenereerd, zijn de detectiekastjes het WPS-signaal alweer vergeten (real-time conversie zonder opslag van WPS-informatie).

Stap 3 – De detectiekastjes sturen hun gehashte informatie door naar de centrale virtuele telmachine. Dit is een algoritme die de *stream* aan hashwaarden – denk aan 698H73365, 575H28141, 036H70594, enzovoorts – analyseert aan de hand van door de gemeente gedefinieerde zones zoals een straatdeel of plein. De telmachine houdt er tevens rekening mee dat niet iedereen wifi bij zich draagt of heeft ingeschakeld. De uitkomst van die analyse ontvangt de gemeente als een drukte-indicatie op zone-niveau, dus op een hoger aggregatieniveau. De conversie van gegevens naar informatie op een hoger aggregatieniveau, is eveneens een manier van anonimiseren.

[2] Selectie uit het WPS-signaal spoort met artikel 5.1c AVG (gegevensminimalisatie).

6 AVG-risicobeoordeling

De hier geschetste drievoudige anonimisering garandeert volledige anonimiteit. Hierdoor is uitgesloten dat een passant nadeel kan ondervinden bij opvang van WPS-signalen door de druktemeter (de gemeente schendt niet de privacy).

De druktemeter stelt gebruikers in staat om geïnformeerde keuzes te maken over het wel of niet betreden van een bepaald gebied. Doorredenerend ligt er meer risico besloten in het *niet* voeren van de druktemeter, continuïteitsproblemen of onbetrouwbare drukte-indicaties, dan het wel voeren ervan. Hoe effectief de druktemeter werkelijk is, hangt samen met vraag hoe groot het risico is van coronabesmettingen in de openbare ruimte, maar die discussie valt buiten de scope van de AVG. Baat het niet, schaadt het niet in privacyopzicht. Dat bijvoorbeeld ouderen dankzij de druktemeter zich veiliger kunnen voelen, is ook van waarde.

Een en ander onder de aanname dat de anonimiteitsmaatregelen werkelijk bestaan en goede werking hebben. Mocht de techniek van de druktemeter anders worden ingezet of geconfigureerd, zal opnieuw moeten worden bekeken wat de risico's zijn. Het college heeft dat te bewaken volgens de raamafspraken in het bestuurlijk privacybeleid, om te voorkomen dat er niet alsnog sprake kan zijn van gebrekkige gegevensbescherming, wat een schending zou betekenen van de AVG.

7 Legitimiteit

Het coronavirus is bij ministerieel besluit vastgesteld als een infectierisico in de hoogste risicocategorie. Op basis van de Gemeentewet, de Wet veiligheidsregio's en de Wet publieke gezondheid heeft het college, met name de burgemeester, taken op het gebied van coronabestrijding. De gemeente heeft aan de bevolking informatie te verschaffen over risico's voor de gezondheid en voorzorgsmaatregelen.

De druktemeter is in dit verband een voor de hand liggende informatievoorziening. De privacyvriendelijkheid van de aanpak verhoogt de legitimiteit. De druktemeter dient welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden, die verband houden met de bescherming van de publieke gezondheid, openbare orde en veiligheid en het recht op informatie. Een en ander met respect voor het privéleven en het recht op bescherming van persoonsgegevens.

8 Transparantie en rechten van betrokkenen

De gemeente is transparant over de inzet van de druktemeter, wat onder meer blijkt uit het betrekken van het Stadspanel data en informatieverstrekking aan de gemeenteraad.

Zolang druktemeter functioneert op basis van volledig anonieme gegevensverwerking, rusten er op de gemeente geen informatieverplichtingen in de zin van artikel 13 en 14 AVG. Ook rechten zoals inzage- en correctierechten zijn bij volledig anonieme gegevensverwerking niet aan de orde, net zo min als de meldplicht datalekken volgens artikel 33-34 AVG.

Voor begrip en draagvlak is het verstandig om heldere voorlichting te geven over de werking van de druktemeter en de privacybeschermende eigenschappen ervan. Onderdeel van een dergelijke aanpak kan zijn dat mensen door middel van bordjes of stickers worden geattendeerd op de werking van de druktemeter in een gebied. Dit niet als een waarschuwing (er is immers geen privacyrisico) maar in het kader van de coronabestrijding. Informatie over privacybescherming valt bijvoorbeeld te verstrekken aan de hand van een webpagina die toegankelijk is via een QR-code.

9 Status

De FG wordt in de AVG tot taak gesteld om toe te zien op de naleving van de AVG, gerelateerde wet- en regelgeving en het gegevensbeschermingsbeleid van de gemeente. Dit doet de FG in onafhankelijkheid en waar nodig in samenwerking met de Autoriteit Persoonsgegevens.

FG's dienen te zijn aangewezen op grond van hun professionele kwaliteiten, in het bijzonder hun deskundigheid op het gebied van het gegevensbeschermingsrecht en de praktijk.

De zienswijze in dit FG-advies vloeit dan ook voort uit toepassing van het (EU) publiekrecht - met name het EU Handvest Grondrechten en de AVG. Met lagere wet- en regelgeving is rekening gehouden voor zover deze met de AVG in overeenstemming zijn. De rechtspraak volgt dezelfde lijn.

Herziening is mogelijk als daarvoor goede argumenten zijn volgens bovenstaande spelregels. Boven de FG staat de rechter. Rechterlijke toetsing is altijd welkom.

Privacy
Management
Partners
Coöperatie UA
adres
Vondellaan 58
3521 GH Utrecht
telefoon
+31 85 401 38 66
e-mail
info@pmpartners.nl
website
www.pmpartners.nl