AUTORITEIT
PERSOONSGEGEVENS

Smart Cities

Onderzoeksrapport bescherming van persoonsgegevens in de ontwikkeling van Nederlandse Smart Cities

Juli 2021

Over de Autoriteit Persoonsgegevens
Iedereen heeft recht op een zorgvuldige omgang met zijn persoonsgegevens. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving.

Voorwoord

Steeds vaker worden door gemeenten persoonsgegevens verzameld in de openbare ruimte met smart city-toepassingen. Bij de term smart cities blijf ik vaak hangen op het woord 'smart', want wat betekent een smart city? Met welk doel en voor wie moet de openbare ruimte slim zijn? Inzet van technologie kan gemeenten meer inzicht geven in het gebruik van de openbare ruimte of zorgen voor nieuwe manieren om het gebruik van de openbare ruimte te sturen. Daarom is het belangrijk om stil te staan bij de prijs die u en ik betalen wanneer wij ons in zo'n smart city bevinden. Hoe verhoudt het verzamelen van onze persoonsgegevens in de openbare ruimte zich tot onze vrijheid? Data kan gebrekkig zijn, ambigu, of kan zelfs discrimineren. Het gevaar bestaat dat dataïsme en digitale solutionisme de overhand krijgen: het geloof dat alles is te vatten in data en met technologie beheersbaar is. Zeker in de openbare ruimte, waar de hoeveelheid mensen even groot als divers is, is het maar de vraag of dit zich laat vatten in data laat staan zich er daarvoor laat beheersen. Het gevaar bestaat dat we naar een surveillancemaatschappij gaan waar je niet meer ongedwongen op straat kunt lopen. Om die reden pleiten wij daarom ook om een verbod op gezichtsherkenning in de openbare ruimte.[1]

Met dit rapport wijzen wij op het belang van een openbare ruimte waarin burgers zich vrij en onbespied kunnen bewegen. Wij roepen bestuurders en ambtenaren op om stil te staan bij de rechten en vrijheden van burgers en die ook daadwerkelijk mee te nemen bij elke stap in de ontwikkeling naar een smart city. En zich daarbij bewust te zijn dat een gemeente niet zomaar inbreuk mag maken op het grondrecht van gegevensbescherming van burgers, maar daarvoor een wettelijke basis nodig heeft of vrije toestemming van burgers. Laat privacy het startpunt zijn van innovatie, niet het sluitstuk.

Gemeenteraadsleden wil ik specifiek meegeven om u te verdiepen in het (ethisch) kader bij ieder technologisch voorstel en te wegen of dat voorstel de rechten en vrijheden van burgers respecteert. Vraag ook advies aan de Functionaris voor gegevensbescherming. Zorg ervoor dat u zorgvuldig, compleet en vanuit meerdere invalshoeken tot uw afweging komt. Niet om een AVG-vinkje te zetten, maar omdat u het beste wilt voor de inwoners en bezoekers van uw gemeente en verantwoorde innovatie wilt stimuleren. Want uiteindelijk is het niet de technologie maar de mens die de openbare ruimte slim maakt.

Monique Verdier
Vicevoorzitter Autoriteit Persoonsgegevens

[1] https://autoriteitpersoonsgegevens.nl/nl/nieuws/privacytoezichthouders-pleiten-voor-verbod-op-gezichtsherkenning

Inhoudsopgave

1. Samenvatting

De openbare ruimte wordt in toenemende mate onderworpen aan de inzet van technologie. Denk aan wifi- en bluetoothtracking, (mobiele of gedragen) camera's of sensoren die data verzamelen over verkeer of geluid. Gemeenten benutten deze technologie steeds vaker om meer inzicht te krijgen in de openbare ruimte om deze te kunnen optimaliseren, beïnvloeden of beter te kunnen beheren. Deze smart city-toepassingen kunnen daarbij persoonsgegevens in of over de openbare ruimte verwerken. Verschuiving van doelen, middelen, en daarmee dus de inzet van persoonsgegevens voor andere doeleinden dan oorspronkelijk bedoeld komt regelmatig voor en vormt een potentiële bedreiging voor de grondrechten van personen die zich in de openbare ruimte begeven. Tevens bestaat het risico dat kennis over de openbare ruimte wordt ingewisseld voor data over de openbare ruimte; data die gebrekkig kan zijn, ambigu kan zijn, of kan discrimineren. De AP heeft daarom onderzoek gedaan naar de bescherming van persoonsgegevens bij de ontwikkeling en inzet van smart city-toepassingen door gemeenten.

De AP constateert dat er grote verschillen bestaan in de inzet van smart city-toepassingen. Waar een groep gemeenten voorop loopt in de ontwikkeling van smart city-toepassingen, zijn er ook gemeenten die (nog) geen of beperkt smart city-toepassingen in de openbare ruimte inzetten. Dit verschil lijkt sterk beïnvloed te worden door specifieke vraagstukken en door grootte, verstedelijking en bevolkingsdichtheid van de gemeente. Het verschil tussen gemeenten uit zich in zowel het aantal toepassingen als het innovatieve karakter van de gekozen technologie voor de toepassingen. Het grootste gedeelte van de toepassingen is gericht op mobiliteit en (verkeers)veiligheid, variërend van het meten van bezoekers- en verkeersstromen tot het monitoren van uitgaansgebieden.

Om smart city-toepassingen verantwoord verder te ontwikkelen dienen vrijwel alle gemeenten meer kennis te ontwikkelen en aandacht te besteden aan specifieke gemeentelijke kaders en een sterker bewustzijn over de gevolgen van smart city-toepassingen op rechten en vrijheden van burgers, waaronder de bescherming van persoonsgegevens. De inzet van het meten van persoonsgegevens in de openbare ruimte is aan strenge eisen gebonden. Niet altijd is de vaststelling of de verwerkingen rond de smart city-toepassing wel rechtmatig zijn in voldoende mate onderbouwd of gedocumenteerd. Dit start bij de vraag of het verzamelen van persoonsgegevens in de openbare ruimte door een gemeente wel rechtmatig is. Daarbij moeten gemeenten gemaakte afwegingen over de verwerking van persoonsgegevens bij smart city-toepassingen ook goed vastleggen, bijvoorbeeld in DPIA's, en deze ook bijwerken. Pas wanneer de rechtmatigheidsvraag positief is beantwoord, is het verstandig ook te kijken naar ethische vraagstukken.

De smart city is meer dan de som der toepassingen. Waar een smart city-toepassing afzonderlijk nog niet zo spannend of risicovol lijkt, kan het geheel van toepassingen wel degelijk zorgen voor grotere of nieuwe risico's. Een helder gemeentelijk beleid, democratische controle en het betrekken van burgers kan helpen bij het controleren van risico's en verantwoord ontwikkelen van smart city-toepassingen. Transparantie is hiervoor noodzakelijk. De inzet van technologie in de openbare ruimte is immers een zwaarwegend besluit waarbij alle aspecten zorgvuldig afgewogen dienen te worden. Niet alles hoeft of kan immers met technologie of data opgelost te worden. Om de juiste vragen te stellen en burgers centraal te stellen bij het bepalen van het doel van smart city-toepassingen kan een ethisch kader behulpzaam zijn. In het onderzoek bleek in groeiende mate aandacht voor ethiek in de ontwikkeling van smart city-toepassingen, bijvoorbeeld door het aanstellen van een (ethische) commissie. Deze dient wel op een concrete wijze onderdeel uit te maken van het ontwikkelproces, anders bestaat het risico dat de burger niets merkt van deze goedbedoelde gesprekken.

Op basis van het onderzoek komt de AP tot de volgende aandachtspunten voor gemeenten:

- Basisbeginselen van de AVG moeten op orde zijn. Stel vast of de wijze waarop persoonsgegevens worden verwerkt rechtmatig is. Wat is het concrete doel van de inzet van smart city-toepassing en welke rechtmatige grondslag bestaat er voor de gegevensverwerking? En is het echt noodzakelijk om persoonsgegevens te verwerken om het doel te bereiken? Als er geen grondslag is voor de verwerking of als de gegevensverwerking niet noodzakelijk is voor het vastgestelde doel, dan mag de smart city-toepassing niet worden ingezet. Doelverschuiving is een reëel risico dat de rechten en vrijheden van burgers kan schaden.
- DPIA als proces. Het opstellen van een DPIA is een belangrijk proces om te beoordelen of de verwerking van persoonsgegevens bij smart city-toepassingen rechtmatig en behoorlijk is, welke risico's er zijn en om intern en extern verantwoording af te leggen over de gemaakte keuzes. Het opstellen van een DPIA voor smart city-toepassingen die persoonsgegevens verwerken is vaak verplicht. Er zijn verbeterpunten voor gemeenten bij het opstellen van de DPIA's. Gemeenten zouden DPIA's bij smart city-toepassingen vaker kunnen publiceren om verantwoording af te leggen over datavergaringen in de openbare ruimte.
- Grip op de smart city. In plaats van het vaststellen van de kaders voor gegevensbescherming (en ethiek) per smart city-toepassing, dienen gemeenten beleid te ontwikkelen voor de inzet van smart city-toepassingen. Deze moet ook worden vertaald naar concrete handvatten voor de praktijk, dit gebeurt nog niet altijd. Daarnaast hebben gemeenten ook een rol in het verkrijgen van inzicht in de sensoren die door derden in de openbare ruimte worden geplaatst. Gemeenten kunnen de mogelijkheid en wenselijkheid onderzoeken om gemeentelijke voorwaarden te verbinden voorafgaand aan de inzet van sensoren in de openbare ruimte door derden.
- Gemeenteraad als tegenmacht. Digitalisering en de inzet van smart city-toepassingen verdienen meer aandacht bij de gemeenteraad. Gemeenteraden moeten voldoende kennis en informatie daarover krijgen om hun democratische taak goed uit te kunnen voeren. Het betrekken van experts kan helpen om de juiste vragen te stellen.
- Privacy in de haarvaten. Veel gemeenten organiseren nog onvoldoende privacy in de uitvoering van hun werkzaamheden. Het vrijmaken van voldoende mensen en middelen en het goed positioneren van privacyprofessionals in de organisatie is essentieel. In het bijzonder dient daarbij aandacht te zijn voor de FG, die een specifiek takenpakket met bescherming heeft om diens rol te kunnen uitoefenen. Dit draagt bij aan een positief ontwikkelklimaat waarin toepassingen volgens het privacy by design principe worden ontwikkeld.
- Oplossing of probleem. Gemeenten, zeker indien zij onvoldoende kennis hebben van verwerkingen van persoonsgegevens, gaan soms te snel in zee met leveranciers van 'mooie oplossingen'. Wees kritisch ten aanzien van uitlatingen van een leverancier ten aanzien van het voldoen aan de AVG of de stelling dat er geen persoonsgegevens worden verwerkt.
- Burgers als brein. De echte kennis over de openbare ruimte zit bij de gebruikers daarvan. Burgers kennen niet alleen de problemen, maar zien vaak andere risico's van het verwerken van persoonsgegevens in of over de openbare ruimte. De AP ziet bij risicovolle smart city-toepassingen in de praktijk niet hoe de gemeente alle risico's voorafgaand in kaart kan brengen zonder de burgers om hun mening te vragen. Het betrekken van burgers lijkt in smart city-toepassingen een sleutel tot succes, echter wordt dit nog maar zelden uitgevoerd.

Pas als aan deze aspecten aandacht wordt besteed is verantwoorde verdere ontwikkeling van de smart city mogelijk. Zonder aandacht voor deze aspecten loopt de Nederlandse smart city het risico om de burger uit het oog te verliezen en zelfs de rechten en vrijheden van het individu te bedreigen. Dit risico geldt juist in de openbare ruimte, waarin burgers zich vrij en onbespied moeten kunnen wanen.

2. Inleiding

De Autoriteit Persoonsgegevens (AP) heeft in de Focus 2020-2023 digitale overheid als één van de drie focusgebieden bestempeld. Smart cities is hierin een belangrijk aandachtsgebied vanwege de groeiende inzet van datagedreven toepassingen die persoonsgegevens verwerken in de openbare ruimte. Deze toepassingen zitten veelal in nog de ontwikkelings- of groeifase, waarbij ook vragen rondom de bescherming van persoonsgegevens een belangrijke rol spelen.

De AP heeft vanuit dit aandachtsgebied besloten een onderzoek te starten naar smart city-toepassingen door gemeenten om de omgang met persoonsgegevens in de Nederlandse smart city in kaart te brengen. Hiermee beoogt de AP duurzame innovatie, waarbij de privacy van betrokken burgers in smart cities is gewaarborgd, te stimuleren. De AP wil met dit onderzoek onder andere inzicht verkrijgen in het gebruik van persoonsgegevens in smart city-toepassingen, de inzet van de gegevensbeschermingseffectbeoordeling (DPIA), de rol van de Functionaris voor Gegevensbescherming (FG), en ervaringen van gemeentes en experts. Daarvoor heeft de AP bij 12 Nederlandse gemeenten documentatie opgevraagd en een vragenlijst voorgelegd. Ook zijn er interviews gehouden met wethouders, FG's, betrokken ambtenaren en experts. Het doel van dit onderzoek is niet geweest om mogelijke overtredingen op te sporen, maar om inzicht te verkrijgen en deze constateringen te delen om duurzame innovatie te stimuleren. De verkregen inzichten deelt de AP met dit rapport.

In dit rapport gaan we in op de opzet van het onderzoek, de relevante basisbeginselen uit de Algemene verordening gegevensbescherming (AVG) in het kader van smart cities, de DPIA's die de AP heeft bestudeerd in het kader van dit onderzoek, op welke wijzen de gemeenteraad en het college grip kan houden op de smart city en de rol van burgers, het belang van de privacyorganisatie van gemeenten, Mobility as a Service en sluiten we af met aanbevelingen en een conclusie over de stand van zaken betreffende gegevensbescherming in de Nederlandse smart city.

2.1 Definitie smart city

Onder een smart city-toepassing verstaat de AP het verzamelen en verwerken van (persoons)gegevens over of in de openbare ruimte door de inzet van sensoren, technologie of andere toepassingen om inzicht in, of analysemogelijkheden over de openbare ruimte te verkrijgen, of sturing van de openbare ruimte mogelijk te maken. Er bestaat een breed scala aan smart city-toepassingen die mogelijk onder deze definitie vallen. Te denken valt aan de inzet van wifi- en bluetoothtracking, inzet van (mobiele of gedragen) camera's, of sensoren die data verzamelen over verkeer of geluid. De AP gebruikt smart city als term die alle openbare ruimte in Nederland omvat, ook dorpen, natuur en agrarische gebieden.

2.2 Doel onderzoek

Het doel van dit onderzoek is meerledig. Op basis van het onderzoek wil de AP:

- inzicht verkrijgen in de verwerkingen van persoonsgegevens binnen smart city-toepassingen;
- de inzet van de DPIA als middel onderzoeken, stimuleren, en daarbij de voorafgaande raadpleging in de zin van artikel 36 van de AVG onder de aandacht brengen;
- best practices over smart city-toepassingen verzamelen en delen;
- de rol van de FG bij de ontwikkeling van smart city-toepassingen onderzoeken;
- privacyvriendelijke innovatie stimuleren in het gehele proces van ontwikkeling van smart city-toepassingen;

- het bewustzijn bij gemeenten vergroten dat smart city-toepassingen grote risico's voor de rechten en vrijheden van het individu met zich mee kunnen brengen.

Bij het onderzoek is de focus gelegd op smart city-toepassingen waarbij de gemeente optreedt als verwerkingsverantwoordelijke. Daarnaast hebben we in het kader van dit onderzoek ook aandacht besteed aan de regulering van smart city-toepassingen door gemeenten (bijvoorbeeld private partijen die sensoren in de openbare ruimte inzetten) en samenwerkingsverbanden.

2.3 Aanpak

Om bovenstaande doelen te bereiken zijn 12 gemeenten in twee groepen onderzocht. De eerste groep betrof vijf gemeenten in meer stedelijke gebieden. De tweede groep betrof zeven gemeenten met een meer diverse ligging en verschillende samenstelling in Nederland. Er is gekozen voor een groep waarbij gemeenten zijn geselecteerd die zich profileerden als smart city of door het hebben van smart city-beleid, en gemeenten waarbij dit niet bekend was en die een doorsnee representeren van bijvoorbeeld een middelgrote gemeente of kleine gemeente. Smart cities worden snel geassocieerd met de grote steden of de Randstad, maar speelt ook bij kleinere gemeenten in Nederland. Bij deze 12 gemeenten is een overzicht van smart city-toepassingen opgevraagd, de bijbehorende DPIA's, en is gevraagd een vragenlijst in te vullen, die te vinden is in de bijlage bij dit rapport. Op basis daarvan zijn in een aantal gevallen vervolgvragen gesteld en interviews met wethouders, ambtenaren en FG's gehouden. Ook zijn enkele experts uit wetenschap en praktijk geïnterviewd over specifieke vraagstukken die op het snijvlak van technologie, ethiek en bestuur spelen in smart cities.

De eerste fase van het onderzoek betrof vijf gemeenten en duurde van september 2019 tot februari 2020. De tweede fase van het onderzoek betrof zeven gemeenten en duurde van maart 2020 tot augustus 2020. Gesprekken en interviews zijn gehouden tussen april 2020 en november 2020, waarbij de afronding van het onderzoek vertraging heeft opgelopen door de effecten van COVID-19 op de organisatie.

2.4 Medewerking aan onderzoek

Gemeenten zijn op basis van de AVG en de Algemene wet bestuursrecht (Awb) verplicht om mee te werken aan een onderzoek van de AP.[2] In dit onderzoek heeft de AP informatie meermaals moeten vorderen en in één instantie een normoverdragend gesprek moeten voeren met een gemeente die onvoldoende meewerkte aan het verzoek en de vordering van de AP. Juist publieke organisaties dienen de belangen en grondrechten van de burger te beschermen, transparant te handelen en daartoe ook te voldoen aan verzoeken en vorderingen van de toezichthouder. Dat geldt in dit geval des te meer omdat de opgevraagde informatie grotendeels aanwezig dient te zijn bij gemeenten op grond van de accountabilityverplichtingen uit de AVG.

2.5 Reflecties op het onderzoek en de Nederlandse smart city

Om te stimuleren dat gesprekken tussen alle partijen plaatsvinden, heeft de AP een aantal deskundigen gevraagd om een onafhankelijke reflectie te schrijven op basis van dit rapport en hun visie op elementen van de smart city. Deze deskundigen hebben inzage gekregen in het conceptrapport en zijn gevraagd op basis van hun expertise om een reflectie te schrijven zonder sturing op inhoud. De AP heeft deze reflecties in zijn geheel zonder redactie overgenomen om een onafhankelijke reflectie mogelijk te maken. Er is geen vergoeding of tegenprestatie verstrekt aan de schrijvers of organisaties. De inhoud van deze reflecties is onafhankelijk geschreven en is niet getoetst of goedgekeurd door de AP en dient ook niet als zodanig te worden gelezen.

[2] Artikel 5:20, eerste lid, Awb jo. artikel 31 AVG.

3. Basisbeginselen AVG voor de smart city

Steden, stedelijke gebieden en gemeenten zijn steeds vaker op zoek naar slimme oplossingen voor vraagstukken op het gebied van onder andere mobiliteit, energie, veiligheid en huisvesting. Deze slimme oplossingen worden gevonden in sensoren en data. Ondersteund door technologieën zoals machine learning kunnen gemeenten data verzamelen of data combineren over bijvoorbeeld bezoekersstromen, verkeer of veiligheid. Door gebruik van de data kunnen bewoners worden 'verleid' tot betere keuzes en kunnen gemeenten het gebruik van de openbare ruimte optimaliseren.

De inzet van slimme oplossingen in de openbare ruimte raakt ontegenzeggelijk aan een aantal grondrechten. Zo kan het gebruik van data voor het indelen of uitsluiten van (groepen) mensen op basis van gedrag of uiterlijke kenmerken leiden tot discriminatie. Het verwerken van persoonsgegevens is per definitie een inbreuk op het recht op gegevensbescherming. De ontwikkeling van smart cities raakt ook aan ethische aspecten en maatschappelijke vraagstukken. Vragen die gemeenten zich in dit kader kunnen stellen zijn bijvoorbeeld de volgende: Kunnen problemen in complexe ecosystemen zoals steden bijvoorbeeld wel worden opgelost met data, als de vergaarde data per definitie beperkt is en niet objectief? Sluit het gebruik van data alternatieve oplossingsrichtingen uit? Kan je je in een smart city nog vrij voelen of afwijkend gedrag vertonen?

Om duurzame innovatie te stimuleren waarbij de grondrechten van het individu serieus worden afgewogen en burgers centraal staan, dient elke gemeente bij elke verwerking een aantal basiselementen op orde te hebben om tot een rechtmatige verwerking van persoonsgegevens te komen. Deze inbreuk dient niet lichtzinnig gemaakt te worden. Aan de inzet van gegevensverwerking in de openbare ruimte zijn strenge eisen verbonden. De verwerking van persoonsgegevens kan enkel rechtmatig plaatsvinden als daarvoor een rechtmatige grondslag is. In dat licht is het daarom belangrijk om, voordat we dieper ingaan op de resultaten van dit onderzoek, stil te staan bij een aantal van deze basiselementen.

3.1 Rechtmatigheid

De AVG bepaalt aan de hand van open normen in welke gevallen een verwerking van persoonsgegevens, zoals door middel van smart city-toepassingen, rechtmatig is. Een gegevensverwerking is rechtmatig als aan ten minste één van de grondslagen genoemd in de AVG is voldaan. Het doel van de verwerking bepaalt welke grondslag van toepassing is. Daarom moet steeds voorafgaand aan de start van de gegevensverwerking worden bepaald wat het doel is van de smart city-toepassing en of een verwerking van persoonsgegevens met die toepassing rechtmatig is. Als er geen grondslag is voor de verwerking van persoonsgegevens, dan kan de smart city-toepassing niet worden ingezet. Zelfs niet als een smart city-toepassing wel persoonsgegevens verwerkt, maar het niet het doel is om persoonsgegevens te verwerken: ook dan wordt immers een inbreuk gemaakt op een grondrecht.

Een grondslag die voor gemeenten specifiek van belang is voor de verwerking van persoonsgegevens in de openbare ruimte is "de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag (artikel 6 lid 1 sub e AVG)". Gemeenten mogen met andere woorden alleen gegevens verwerken in het kader van de uitoefening van hun taken als de wetgeving deze daartoe passende bevoegdheden heeft gegeven. Gemeenten hebben bijvoorbeeld de publieke taak om de openbare ruimte te beheren. Deze algemene taak alleen is echter niet voldoende om daarvoor persoonsgegevens te mogen verwerken. De AVG eist namelijk dat wetgeving op basis waarvan verwerkingen voor een publieke taak plaatsvinden voldoende concreet en voorzienbaar is. Gemeenten moeten dus een voldoende precieze

wettelijke grondslag kunnen aantonen; een algemene taakomschrijving is daarvoor vaak onvoldoende. Wat precies 'voldoende voorzienbaar' is, zal per geval moeten worden afgewogen. In de openbare ruimte is het vrijwel niet mogelijk om van individuele burgers toestemming te vragen. Dit betekent dat de grondslag toestemming vrijwel niet bruikbaar is voor smart city-toepassingen.[3]

Voor de beantwoording van de vraag of er voor de verwerking een grondslag bestaat moet een gemeente ook aan kunnen tonen dat een verwerking van persoonsgegevens noodzakelijk is voor het doel dat wordt nagestreefd. Hierbij dient de gemeente af te wegen of er minder ingrijpende alternatieven voorhanden zijn, en of de inbreuk wel opweegt tegen het doel dat verwezenlijkt wordt, waarover meer verderop in dit hoofdstuk. Dit vereist een goede afweging, die moet worden gemaakt (en gedocumenteerd) voordat de verwerking van persoonsgegevens start.

Pas wanneer er een rechtmatige grondslag aanwezig is, kan een gemeente persoonsgegevens verwerken. Zonder rechtmatige gegevensverwerking kunnen smart city-toepassingen niet ontwikkeld of toegepast worden. Dit geldt ook voor pilots. Het enkele feit dat de verwerking rechtmatig is, betekent echter niet dat een smart city-toepassing zomaar kan worden ingezet. Uit de AVG volgen nog diverse verplichtingen waaraan de verwerking van persoonsgegevens moet voldoen. De belangrijkste verplichtingen komen in dit rapport aan de orde.

Aanbeveling: Bepaal voordat je aan enige smart city-toepassing begint of er persoonsgegevens worden verwerkt en of de verwerking van persoonsgegevens rechtmatig is. Zonder rechtmatige gegevensverwerking kunnen smart city-toepassingen niet ontwikkeld of toegepast worden.

3.2 Doelbinding

Het komt bij smart city-toepassingen niet zelden voor dat deze in eerste instantie worden ingezet als oplossing voor een bepaald doel, maar later ook als 'handig' worden gezien voor de oplossing van andere (beleids)doelen. Dit staat op gespannen voet met het doelbindingsprincipe. Doelbinding bestaat uit twee elementen: doelen moeten welbepaald, goed omschreven en gerechtvaardigd zijn en gegevens mogen niet verder worden verwerkt op een met die doelen onverenigbare wijze. Een voorbeeld is de inzet van camera's voor handhavingsdoeleinden, waarbij de beelden later ook worden gebruikt voor druktemetingen. Dit kan alleen wanneer het nieuwe doel verenigbaar is met het oorspronkelijke doel waarvoor de gegevens zijn verzameld en verwerkt. Bij elk nieuw doel, nieuw proces of inzet van nieuwe technologie zal opnieuw moeten worden getoetst door gemeenten of de nieuwe doelen passen bij de oorspronkelijke doelen van de gemeente. De verwachting van de burger zullen hierbij ook een rol spelen; hoe minder deze in redelijkheid kan voorzien dat zijn persoonsgegevens ook worden verwerkt voor het andere doel, hoe minder snel de gegevensverwerking verenigbaar zal zijn met het oorspronkelijke doel.

3.3 Noodzakelijkheid

Een verwerking van persoonsgegevens kan alleen noodzakelijk zijn als de smart city-toepassing daadwerkelijk een bijdrage levert aan vooraf vastgestelde, concrete doelen en het nagestreefde doel in verhouding staat tot de aard en hoeveelheid persoonsgegevens die ervoor worden verwerkt (proportionaliteit). Daarbij mag er geen minder inbreukmakend alternatief zijn om hetzelfde doel te bereiken (subsidiariteit). Dit dient gedocumenteerd te worden met heldere en toetsbare onderbouwing in

[3] Zie voor nadere informatie over de grondslag ook: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_ap_gemeente_enschede.pdf, p. 20 e.v. Overigens is toestemming bij overheidsorganisaties ook meestal geen geschikte grondslag omdat toestemming 'vrij' moet worden gegeven. In de relatie tussen overheid en burger is sprake van een machtsverschil, waardoor toestemming niet altijd vrijelijk kan zijn gegeven.

de DPIA, die tevens voldoende actueel moet zijn. Elke verwerking van persoonsgegevens die niet noodzakelijk is, kan niet voldoen aan de AVG.

Het Rathenau Instituut constateerde in een onderzoek naar smart cities dat het essentieel is dat gemeenten experimenten helder afbakenen met duidelijke begin- en einddatum, (meetbare) doelstellingen en indicatoren en evaluatiemomenten vaststellen. Dit vindt in de praktijk lang niet altijd plaats.[4] De AP herkent zich in deze bevindingen en benadrukt dat ook voor smart city-toepassingen die reeds 'in productie' zijn het vaststellen van concrete doelen en het monitoren van de effectiviteit van wezenlijk belang is om te kunnen voldoen aan de AVG. Zo wordt in een toegezonden DPIA van een gemeente in het kader van dit onderzoek over pilots met bodycams als doel genoemd om "[de] veiligheid en hun gevoel van veiligheid bij de uitvoering van primaire taken [te] vergroten. En dat in die situaties de-escalerend kan werken". Vervolgens wordt aangegeven dat de resultaten van de pilot na afloop van een periode van 3 maanden "breed [worden] geëvalueerd". Positief is dat de DPIA een duidelijke begin- en einddatum benoemt, alsmede de verplichting tot evaluatie. Een verbeterpunt is dat uit de toegezonden documentatie niet duidelijk blijkt op basis van welke indicatoren de doeleinden worden gemeten en op basis van welke criteria wordt bepaald of de pilot ook in productie gaat. Dit is zeker van belang om vast te stellen bij 'zachte' doelstellingen als het verbeteren van 'het veiligheidsgevoel'.

Aanbeveling: Stel vast aan welk(e) doel(en) de smart city-toepassing moet bijdragen. Maak deze doelstellingen zo concreet en meet-/toetsbaar mogelijk om de effectiviteit van de smart city-toepassing vast te stellen. Algemene doeleinden als 'veiligheid' of 'leefbaarheid' moeten nader worden ingevuld. Stel ook vast wat de vervolgstappen zijn als een smart city-toepassing niet slaagt of er ongewenste neveneffecten optreden.

3.3.1 Subsidiariteit

Gemeenten zullen voorafgaand aan de inzet van smart city-toepassingen steeds moeten bepalen of er minder inbreukmakende alternatieven zijn om hetzelfde doel te bereiken. Soms zijn (menselijke) interventies of andere technische oplossingen even effectief om hetzelfde doel te bereiken, zonder dat daarbij persoonsgegevens of waarbij minder persoonsgegevens worden verwerkt.[5] Veel aangeboden 'oplossingen' van marktpartijen moeten daarom kritisch worden bezien. Gegevensverwerkingen in smart city-toepassingen dienen immers ondersteunend te zijn en geen doel op zich. Gemeenten moeten bij de aanschaf of ontwikkelingen van smart city-toepassingen telkens motiveren waarom alternatieve oplossingen waarbij geen of minder persoonsgegevens worden verwerkt geen of onvoldoende bijdragen aan de oplossing van het nagestreefde doel. De AP kan gemeenten ook bevragen naar deze motivering.

Met name in tijden van Covid-19 is een trend te zien in de ontwikkeling van allerlei technische oplossingen. Gemeenten zullen zich regelmatig de vraag moeten stellen of deze daadwerkelijk een bijdrage (blijven) leveren in bijvoorbeeld de regulering van drukte en of niet kan worden gezocht in andere oplossingen.

Aanbeveling: Ga voorafgaand aan de inzet van smart city-toepassingen na of er alternatieve oplossingen zijn om het doel te bereiken waarbij geen of minder persoonsgegevens worden verwerkt. Denk na vanuit het probleem en niet vanuit de geboden oplossing.

[4] Rapport Voeten in de Aarde, p. 6.
[5] Zie in dit kader ook: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_ap_gemeente_enschede.pdf, p. 24 en 25.

3.4 Transparantie

Burgers moeten op een goede manier volledig geïnformeerd zijn over de verzameling van persoonsgegevens in de openbare ruimte die zij niet kunnen mijden. De AP neemt waar dat de transparantie bij het ontwikkelen van smart city-toepassingen en smart city-beleid nog moet worden verbeterd. Transparantie is noodzakelijk zodat de gemeente verantwoording aflegt over smart city-toepassingen die zij ontwikkelt en inzet met als doel dat de burger controle houdt over diens persoonsgegevens en diens rechten kan uitoefenen indien nodig. Het vormgeven van transparantie mag niet een sluitpost zijn van het smart city-beleid. Transparantie begint al bij de wijze waarop besluitvorming plaatsvindt, problemen worden geïdentificeerd welke in aanmerking komen voor technologische of datagedreven oplossingen, en bij de processen die een gemeente heeft om aan te vangen met de ontwikkeling. Tijdens de ontwikkeling kan de burger een belangrijke rol vervullen in het proces om algemene en doelgroepspecifieke risico's in kaart te brengen en de problemen scherp te krijgen, waarover later in dit rapport meer.

Na uitrol van smart city-toepassingen bestaat het gevaar dat er een lappendeken van diverse toepassingen ontstaat over een gemeente waar de burger geen overzicht over kan verkrijgen. Hier ziet de AP een zeer belangrijke uitdaging die wordt opgepakt door een aantal gemeenten middels het onderzoeken van instrumenten zoals een openbaar sensorregister, waarover meer in het hoofdstuk 'Regulering door gemeenten en sensorregisters'. Deze initiatieven bouwen voort op de beginselen van de AVG, waaronder het verplichte register van verwerkingen. Ook de privacyverklaring van gemeenten verdient aandacht om alle doelgroepen op een juiste wijze te kunnen informeren. Niet enkel taal kan hier een rol in spelen – denk bijvoorbeeld aan een Engelse vertaling voor toeristen of tijdelijke inwoners – maar deze dient ook in redelijke mate begrijpelijk te zijn voor personen die laaggeletterd zijn of niet thuis zijn in juridische vaktaal.

4. DPIA

In het onderzoek heeft de AP veel aandacht besteed aan de rol van de DPIA. De DPIA is bedoeld als proces aan de hand waarvan *voorafgaand* aan de gegevensverwerking kan worden beoordeeld of de verwerking rechtmatig en behoorlijk is, of er alternatieven zijn en om de risico's in kaart te brengen en waar mogelijk te mitigeren door het treffen van passende maatregelen. Bovendien legt een gemeente intern en extern verantwoording af waarom bepaalde keuzes zijn gemaakt. De DPIA biedt ook tijdens de gegevensverwerking houvast als procesdocument om gegevensbeschermingsrisico's te monitoren en mogelijke wijzigingen aan te brengen in de verwerking, bijvoorbeeld wanneer er een doelverschuiving plaatsvindt. De AP vraagt daarom in het kader van onderzoeken regelmatig naar DPIA's, waarvan de inhoud en kwaliteit een belangrijke indicator kunnen zijn voor de AP.

4.1 DPIA-plicht

Het uitvoeren van een DPIA is verplicht als de risico's van de gegevensverwerking voor de betrokkene 'hoog' zijn. De Europese privacytoezichthouders hebben gezamenlijk negen criteria opgesteld om te beoordelen of de voorgenomen verwerking van persoonsgegevens een hoog privacyrisico oplevert voor betrokkenen. Als vuistregel is het uitvoeren van een DPIA verplicht als de verwerking aan twee of meer van de negen criteria voldoet.[6] In het kader van smart cities zijn vooral de categorieën 'evaluatie of scoretoekenning', 'stelselmatige en grootschalige monitoring', 'grootschalige gegevensverwerkingen' en 'gebruik van nieuwe technologieën' relevant. Projecten binnen het smart city-kader zullen doorgaans onder twee of meer van deze categorieën vallen waardoor het opstellen van een DPIA verplicht is.

De AP heeft daarnaast een lijst van verwerkingen opgesteld waarvoor het uitvoeren van een DPIA verplicht is gesteld. Dit geldt voor onder meer de volgende verwerkingen:

- Grootschalige verwerkingen en/of stelselmatige monitoring van persoonsgegevens die worden gegenereerd door apparaten die verbonden zijn met internet en die via internet of anderszins gegevens kunnen versturen of uitwisselen (*internet of things*). Denk hierbij bijvoorbeeld aan sensoren die stelselmatig het publiek volgen in de openbare ruimte.
- Het delen van persoonsgegevens in of door samenwerkingsverbanden waarin gemeenten of andere overheden met andere publieke of private partijen bijzondere persoonsgegevens of persoonsgegevens van gevoelige aard met elkaar uitwisselen. Informatieknooppunten zijn hiervan een voorbeeld.
- Grootschalige verwerkingen en/of stelselmatige monitoring van openbaar toegankelijke ruimten met camera's, webcams of drones.
- Grootschalig en/of systematisch gebruik van flexibel cameratoezicht, zoals bodycams.
- Grootschalige verwerkingen en/of stelselmatige monitoring van locatiegegevens van of herleidbaar tot natuurlijke personen. Bijvoorbeeld (scan)auto's, telefoons, of verwerking van locatiegegevens van reizigers in het openbaar vervoer.

4.2 Uitvoering van een DPIA

Uit het onderzoek bleek dat een aantal gemeenten werkt met zogenaamde 'pre-DPIA's'. Hierbij wordt aan de hand van een vragenlijst bepaald of het verplicht is om voor een bepaalde verwerking een DPIA uit te voeren. Een dergelijke vragenlijst kan een goed en laagdrempelig instrument zijn, maar zoals een FG in gesprek met de AP terecht aangeeft moet het uitvoeren van een dergelijke pre-DPIA er niet toe leiden dat als blijkt dat er geen DPIA nodig is, er niet meer stil wordt gestaan bij de afwegingen die moeten worden

[6] Zie voor meer informatie: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia

gemaakt bij de bescherming van persoonsgegevens. De plicht om de juiste waarborgen te treffen en verantwoording af te leggen geldt immers ook als een DPIA niet vereist is.

Een ander punt van aandacht is dat DPIA's periodiek moeten worden herzien c.q. bijgewerkt. Een voorbeeld van een DPIA die de AP heeft ontvangen betreft een document uit 2016 waarin openstaande actiepunten in zijn opgenomen, waaronder het sluiten van een verwerkersovereenkomst en het consulteren van de OR. Als de actiepunten zijn ondernomen dient ook de DPIA te worden bijgewerkt. Ook bij veranderingen in de geconstateerde risico's is het van belang DPIA's periodiek inhoudelijk te herzien en zo nodig bij te werken. Technologie die ingezet wordt in smart city-projecten ontwikkelt zich immers ook gedurende de looptijd van het project. Ook in de huidige tijd met de Covid-19 maatregelen kunnen de risico-afwegingen anders liggen dan over een aantal maanden of jaren. In het algemeen is het aan te raden om een DPIA periodiek te controleren en indien nodig te herzien om zodoende de bestaande en mogelijke nieuwe risico's te kunnen adresseren. Een goed voorbeeld betreft een gemeentelijke FG die aangaf een aantal DPIA's die zijn uitgevoerd vlak na inwerkingtreding van de AVG momenteel opnieuw te doorlopen, gelet op de termijn herzieningstermijn van drie jaar die de gemeente had bepaald voor de DPIA's.

Aanbeveling: Houd DPIA's actueel om de huidige risico's van de verwerking te kunnen aantonen. Openstaande actiepunten in een verouderde DPIA of het niet documenteren van technische aanpassingen in de verwerking voldoen niet aan de verantwoordingsplicht. Bepaal beleid waarbij DPIA's periodiek worden herzien c.q. bijgewerkt.

4.3 Beeld AP ontvangen DPIA's

De AP heeft voor het onderzoek DPIA's opgevraagd over smart city-toepassingen. Van met name de kleinere gemeenten heeft de AP enkele tot geen DPIA's ontvangen. De eerste verklaring hiervoor is dat deze gemeenten simpelweg geen smart city-toepassingen inzetten of enkel smart city-toepassingen inzetten waarbij geen persoonsgegevens worden verwerkt (bijvoorbeeld bij het meten van luchtkwaliteit, vulgraad van containers, detectielussen, etc.). Een tweede verklaring is dat het vaak een verwerking betreft die reeds vóór de AVG werd toegepast en die met inwerkingtreding van de AVG niet is veranderd (voorbeelden zijn kentekenregistraties voor diverse doeleinden, cameratoezicht in openbare ruimtes, etc.). Ten derde geven gemeenten aan dat de risico's van het desbetreffende project niet als 'hoog' kwalificeren en daarom geen DPIA is vereist.

4.3.1 Ontbrekende DPIA's?

Wel stelt de AP in sommige gevallen vraagtekens bij de motivering waarom er geen DPIA is uitgevoerd. Dat is ten eerste het geval bij smart city-toepassingen die in een pilotvorm worden gestart en getest voordat deze breder worden uitgerold. Ook in de pilotfase worden soms al persoonsgegevens verwerkt. De AP benadrukt dat ook verwerkingen van persoonsgegevens in een pilot of proef dienen te voldoen aan de regels van de AVG, waaronder de DPIA-plicht. Hierin dient het doel van de proef te worden beschreven, de grondslag met daarbij de mogelijke uitkomsten en bijbehorende risico's. Een gemeente die aangeeft "[te] onderzoeken of dat de openbare orde taak ex artikel 151c Gemeentewet ook bruikbaar is als grondslag" bij de inzet van (mobiele) camera's als pilot voldoet dus niet aan deze eisen. Daarnaast moet duidelijk worden gemaakt wanneer een proef is geslaagd en wat er gebeurt, bijvoorbeeld met de data, als de proef niet voldoet aan de gestelde eisen en verwachtingen. Ook dient vastgelegd te worden hoe om te gaan met eventuele (niet-)voorziene risico's. Door dit vooraf vast te leggen wordt een helder kader geboden waarbinnen een proef plaatsvindt. Het evalueren van (proef)projecten is tevens van groot belang om doelbinding van (vervolg)projecten te kunnen waarborgen.

Aanbeveling: Smart city-toepassingen die zich in de pilotfase bevinden moeten ook voldoen aan de eisen van de AVG indien daarbij persoonsgegevens worden verwerkt.[7] Ga daarom ook bij pilot- en proefprojecten na in hoeverre deze projecten AVG-compliant zijn en voer zo nodig een DPIA uit.

Ten tweede geven sommige gemeenten aan dat in het kader van bepaalde smart city-toepassingen wordt gewerkt met anonieme gegevens, terwijl de omschrijving van de toepassing soms anders suggereert. Zo geeft een gemeente aan dat via een bepaalde app locatiegegevens van gebruikers worden verwerkt voor een stoplichtsysteem, maar dat "deze niet te herleiden [zijn] naar een persoon of een specifieke smartphone" en "alle verzamelde data anoniem [is]". Gegevens kunnen pas worden beschouwd als anoniem als voor welke partij dan ook, met inzet van (voor het doel) redelijke middelen, het onwaarschijnlijk is hieruit personen te identificeren.[8] Met name bij locatiegegevens is dat bijna ondoenlijk.[9] Ook de juiste toepassing van technologie is noodzakelijk om anonimiteit te waarborgen.[10]

Aanbeveling: Wees kritisch bij het beoordelen van de anonimiteit van de gegevens die worden verwerkt; gegevens kunnen pas worden beschouwd als anoniem als voor welke partij dan ook, met inzet van (voor het doel) redelijke middelen, het onwaarschijnlijk is hieruit personen te identificeren.

Een derde aandachtspunt signaleert de AP in het kader van samenwerkingsverbanden. Smart city-toepassing worden bij samenwerkingsverbanden vaak voor meerdere, uiteenlopende doelen ingezet en vallen onder meerdere wettelijke kaders doordat de gegevens met verschillende partijen binnen en buiten de gemeente worden gedeeld. Te denken valt aan een samenwerking met de politie en private partijen zoals woningcorporaties. Voor de uitwisseling van de gegevens is het noodzakelijk dat van tevoren voldoende duidelijk is of deze uitwisseling rechtmatig is en onder welke voorwaarden partijen de gegevens mogen verwerken en deze vast te leggen.[11] Denk bijvoorbeeld aan het vaststellen welke partij welke gegevens mag verwerken op basis van bepaalde grondslagen, voor welk doel en hoe lang deze gegevens mogen worden bewaard. Te vaak lijkt het nog te gebeuren dat gemeenten en andere aangesloten partijen dit soort vraagstukken willen 'verkennen' tijdens een pilot. Bij een aantal gemeenten waar in samenwerkingsverbanden wordt gewerkt is de DPIA niet altijd aanwezig of afgerond bij de start van de verwerking. Daarnaast blijkt uit enkele DPIA's dat er onduidelijkheden bestaan over de verantwoordelijkheden van de verschillende partijen die betrokken zijn bij de smart city-toepassing en dat een DPIA (daardoor) ontbreekt. De AP benadrukt dat het zaak is om *voorafgaand* aan de gegevensverwerking bij een smart city-toepassing de verantwoordelijkheden helder te beleggen en te documenteren zodat de gegevensuitwisseling 'by design' rekening houdt met de bescherming van persoonsgegevens. Partijen moeten immers weten wie waarvoor verantwoordelijk is en burgers moeten weten bij wie zij hun rechten kunnen uitoefenen; transparantie geven aan burgers over de verwerking en de betrokken partijen is daarom essentieel.[12]

---

[7] Zie ook: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/verantwoordingsplicht#is-de-avg-van-toepassing-bij-pilots-testen-en-proefprojecten-8161.

[8] Rondom anonimisering bestaan veel misverstanden. In een korte factsheet van toezichthouders worden veelvoorkomende misverstanden genoemd en nader uitgelegd: https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf.

[9] Zie ook: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/anonimiteit_en_geaggregeerde_telecomdata.pdf

[10] Zie ook: https://autoriteitpersoonsgegevens.nl/nl/nieuws/techblogpost-praktische-problemen-bij-het-afknippen-van-hashes

[11] Zie ook het onderdeel 'samenwerkingsverbanden' in dit rapport.

[12] De Europese gegevensbeschermingsautoriteiten hebben (vernieuwde) richtlijnen ("Guidelines 07/2020 on the concepts of controller and processor in the GDPR") in consultatie gebracht over de begrippen verwerkingsverantwoordelijke en verwerker. Deze kunnen helpen om de rolverdeling in kaart te brengen in samenwerkingsverbanden.

Aanbeveling: Stel bij samenwerkingsverbanden voorafgaand aan de start van de verwerking vast wie waarvoor verwerkingsverantwoordelijk dan wel verwerker is. Wees daarover ook transparant naar burgers.

4.3.2 Kwaliteit DPIA's

De DPIA's die de AP wel heeft ontvangen bleken tussen, maar soms ook binnen gemeenten van wisselende opzet en kwaliteit. Het verschil in kwaliteit blijkt bijvoorbeeld in het ontbreken van een heldere analyse in een aantal DPIA's over welke gevolgen de verwerking heeft op de rechten en vrijheden van betrokkenen en de waarborgen die (per risico) worden getroffen om de risico's zoveel mogelijk te beperken. Ook werd niet in alle gevallen een duidelijke beschrijving gegeven van de verwerkingen van persoonsgegevens bij een smart city-toepassing, maar werd enkel verwezen naar de werking van een smart city-toepassing. De Europese privacytoezichthouders hebben criteria vastgesteld die gemeenten kunnen gebruiken om te beoordelen of een DPIA volledig genoeg is om aan de AVG te voldoen.[13] Over het algemeen leken de oudere DPIA's van mindere kwaliteit dan de meer recentere. Dit kan allereerst mogelijk worden verklaard doordat in de AVG duidelijkere eisen zijn vastgelegd over de inhoud van de DPIA. Daarnaast speelt mogelijk ook het groeiende niveau van 'privacyvolwassenheid' van gemeenten een belangrijke rol in de kwaliteit van de opgestelde DPIA's. Een volwassen organisatie waarbinnen privacy van burgers een bekend en verankerd begrip is dat op een serieuze wijze wordt meegenomen in het ontwikkelproces draagt in hoge mate bij aan de kwaliteit van een DPIA en de toepassing. Zie ook hoofdstuk 8 van dit rapport voor meer informatie over de privacyorganisatie in de gemeente.

4.4 Voorafgaande raadpleging

De AP heeft via verschillende kanalen kennisgenomen van een aantal smart city-toepassingen die zich in opstartende- of pilotfase bevinden en waar mogelijk hoge (rest)risico's aan zijn verbonden. De AP wijst erop dat een DPIA voorafgaand aan de verwerking van persoonsgegevens moet worden uitgevoerd. Indien de gemeente naar aanleiding van de DPIA bepaalt dat er sprake is van hoge risico's die niet kunnen worden beperkt tot een acceptabel niveau ('hoge restrisico's'), dient er een voorafgaande raadpleging bij de AP in de zin van de AVG te worden ingediend.[14] Tot die tijd kan de verwerking van persoonsgegevens (en daarmee de smart city-toepassing) niet starten. De AP heeft maximaal 8 weken de tijd om een voorafgaande raadpleging te beoordelen en eventueel te voorzien van een advies.[15] Voor complexe verwerkingen is een verlenging van de termijn met 6 weken mogelijk. Als partijen gebonden zijn aan deadlines, bijvoorbeeld omdat de smart city-toepassing wordt ingezet bij geplande evenementen, dan is het van belang dat partijen tijdig de risico's in kaart brengen door middel van een DPIA. De FG kan adviseren of een voorafgaande raadpleging moet worden ingediend bij de AP.

Aanbeveling: Stel het uitvoeren van een DPIA niet uit, maar doe dit zo vroeg mogelijk bij de ontwikkeling van smart city-toepassingen. Zeker bij geplande evenementen of andere toepassingen met deadlines is dat van groot belang. Zo kan tijdig worden bepaald of een verwerking eventueel voor voorafgaande

[13] Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679

[14] Bij de verwerking van politiegegevens geldt een lagere drempel om een voorafgaande raadpleging in te dienen. Een voorafgaande raadpleging is in dat geval ook verplicht als de aard van de verwerking, in het bijzonder met gebruikmaking van nieuwe technologieën, mechanismen of procedures, een hoog risico voor de rechten en vrijheden van de betrokkene met zich meebrengt (art. 33b, eerste lid, onder a Wet politiegegevens). Dit kan van belang zijn in samenwerkingsverbanden waarbij politiegegevens worden verwerkt.

[15] Zie voor meer informatie: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#hoe-beoordeel-ik-of-er-een-restrisico-is-6808

raadpleging moet worden ingediend bij de AP. Betrek de FG zo vroeg mogelijk, zodat deze tijdig kan voorzien van advies.

Wanneer is sprake van een hoog restrisico?
Regelmatig krijgt de AP de vraag wanneer sprake is van een hoog restrisico. Hier is geen eenduidig antwoord op te geven; de risico's zullen per verwerking in kaart moeten worden gebracht. Het is aan de verwerkingsverantwoordelijke om, met de kennis van de omstandigheden van het geval, de risico's te classificeren. Die risico's dienen te worden gemitigeerd door de verwerking zodanig in te richten dat de risico's zo minimaal mogelijk zijn met redelijke middelen en er maatregelen zijn getroffen om de zowel de kans op, als het effect van, een inbreuk op het recht op bescherming van persoonsgegevens te verkleinen. Procedures hoe te handelen indien een risico zich in de praktijk toch voordoet (en bijvoorbeeld resulteert in een datalek) vallen hier ook onder. Met behulp van een aantal richtlijnen kan worden beoordeeld of de risico's na de maatregelen nog classificeren als 'hoog'. De verwerkingsverantwoordelijke beoordeelt of er sprake is van hoge restrisico's. In de praktijk gaat het bij verwerkingen met een hoog restrisico om (grootschalige) verwerkingen waarvoor reeds een DPIA-verplichting geldt omdat de risico's in zijn algemeenheid als hoog worden ingeschat en die inherent aan de verwerking zijn. Denk aan het geval dat de gebruikte data of techniek dusdanig grote inherente risico's kent dat de kansen of effecten groot of niet te voorzien zijn. Zeker bij verwerkingen van de overheid, die betrekking hebben op een grote groep mensen, zijn de effecten al snel hoog. Een restrisico is ook aanwezig indien de kansen of effecten te voorzien zijn, maar er onvoldoende maatregelen voorhanden zijn om deze te adresseren. Een mogelijk restrisico is bijvoorbeeld de kans op vals positieven bij de inzet van algoritmische systemen en de stigmatiserende gevolgen die dat kan hebben bij inzet van een bepaalde technologie.

4.5 Openbaarheid DPIA

Verantwoording dient niet alleen naar de AP, maar vooral naar burgers te worden afgelegd van wie de persoonsgegevens worden verzameld (transparantie) en naar andere geïnteresseerde partijen. De AP juicht het openbaar maken van (delen van) de DPIA over smart city-toepassingen daarom toe, juist omdat smart city-toepassingen worden ingezet in de openbare ruimte. Door als gemeente meer inzicht te geven over de verwerkte persoonsgegevens, de technologie die gebruikt zal worden, mogelijke risico's van de verwerking en de daarvoor genomen maatregelen kan dit bijdragen aan meer vertrouwen in de ingezette toepassingen. Indien gewenst kan bij het openbaar maken van de DPIA mogelijke gevoelige informatie die afbreuk kan doen aan bijvoorbeeld de beveiliging van de verwerking worden weggelaten. In de praktijk zien we dat DPIA's nog niet vaak openbaar worden gemaakt. Het is raadzaam om niet alleen op ad hoc-basis na te denken over de publicatie van DPIA's, maar daarover beleid of afwegingskaders te ontwikkelen. Dit geldt ook voor DPIA's die geen betrekking hebben op smart city-toepassingen.

Aanbeveling: Publiceer zoveel mogelijk de DPIA's van smart city-toepassingen en ontwikkel beleid over de publicatie van DPIA's.

4.6 Betrokkenheid burgers

De AVG bepaalt dat bij de uitvoering van een DPIA "in voorkomend geval de betrokkenen of hun vertegenwoordigers naar hun mening [wordt gevraagd] over de voorgenomen verwerking".[16] In het onderzoek heeft de AP de onderzochte gemeenten daarom opgevraagd of, en zo ja op welke wijze zij burgers betrekken bij de ontwikkeling van smart city-toepassingen. Uit het onderzoek is naar voren gekomen dat gemeenten burgers vaker niet dan wel betrekken bij de ontwikkeling van smart city-toepassingen.

De AP is van mening dat het betrekken van de burger meer voor de hand ligt daar waar de wetgeving een minder duidelijk kader biedt over de inbreuk op de rechten en vrijheden van betrokkenen, bijvoorbeeld omdat de wet niet specifiek bepaalt welke gegevens mogen worden verwerkt en welke waarborgen er moeten worden getroffen. Daar waar de gegevensverwerking van een smart city-toepassing op basis van wet- en regelgeving minder voorzienbaar is, terwijl de mate van inbreuk door de burger wel als hoog kan worden ervaren of hoge risico's voor de rechten en vrijheden van burgers met zich meebrengt/kan brengen, ligt het meer voor de hand burgers te betrekken. Zeker bij smart city-toepassingen ligt het daarom voor de hand om de burger te betrekken. De (gemeentelijke) wet- en regelgeving geeft vrij brede taken voor gemeenten, waardoor niet elke inzet van smart city-toepassing op voorhand te verwachten is.[17] Bovendien kan bijvoorbeeld het volgen van menselijk gedrag met de inzet van smart city-toepassingen als indringend worden beschouwd en mogelijk zelfs tot een *chilling effect* leiden, waarbij mensen zich anders gaan gedragen of de openbare ruimte niet meer willen of durven te gebruiken.

Bij complexe, innovatieve smart city-toepassingen lijkt het welhaast onmogelijk om inzicht te krijgen op de mogelijke inbreuken op de rechten en vrijheden van alle diverse individuen wiens persoonsgegevens verwerkt worden. Om die risico's in kaart te brengen in het kader van de verplichte DPIA is de mening van betrokken burgers van grote waarde. De AVG biedt een zeer geschikt startpunt voor gemeenten om burgers onderdeel te maken van de slimme stad waarin ze leven. Gelet op het feit dat artikel 35 lid 9 AVG betrekking heeft op de DPIA, is het aan te bevelen om in de DPIA op te nemen of, en zo ja op welke wijze de gemeente de betrokkene vraagt naar hun mening. Op deze manier kan bewustwording worden gecreëerd bij de uitvoering en verantwoording worden afgelegd over de vraag in hoeverre de burger (en andere betrokkenen) is gevraagd naar hun mening. Een goed voorbeeld is een gemeente die als standaardvraag in de DPIA heeft opgenomen of de betrokkenen (of hun vertegenwoordigers) gevraagd is om hun visie te geven over de verwerkingsactiviteiten (inclusief motivering van de keuze) en op welke manier opvolging is gegeven aan de visie (en een motivering indien dit niet is gebeurd).

Aanbeveling: Besteed in de DPIA aandacht aan de vraag of betrokkenen naar hun mening is gevraagd en op welke manier er opvolging is gegeven aan deze meningen. Hoe hoger de mogelijke risico's, hoe onduidelijker de wettelijke grondslag of hoe hoger de mate van ervaren inbreuk, hoe meer het voor de hand ligt burgers te betrekken.

[16] Artikel 35, negende lid AVG.
[17] Het zou zelfs tot de conclusie kunnen leiden dat een verwerking niet voldoet aan de rechtmatigheidscriteria (zie het hoofdstuk 'Rechtmatigheid').

5. Reflectie: Participatory DPIAs and administrative law mechanisms in Smart Cities

Auteurs: Athena Christofi†, Jonas Breuer, Olia Kanevskaia†, Ellen Wauters†*
*Organisatie: † imec-CiTiP, KU Leuven; * imec-SMIT, Vrije Universiteit Brussel*
Functies: Onderzoekers, samenwerking in het kader van Smart-city Privacy: Enhancing Collaborative Transparency in the Regulatory Ecosystem (SPECTRE) Project[18]

We warmly welcome this report and the opportunity it provides to understand smart city practices in the Netherlands and reflect on the future. The challenges cities face in becoming smart are similar throughout Europe and the attention and recommendations of the DPA can facilitate learning beyond the Netherlands.

In the following paragraphs we reflect on two issues emerging from the report that we find particularly worthwhile for smart cities and data protection in the EU.

Participatory DPIAs
We welcome the emphasis on the role of citizens in the development of smart-city applications. Citizen participation has a fruitful tradition in other domains and shows promising potential for assessing impacts of data processing in public space. We hope that this emphasis brings together relevant authorities, cities and umbrella associations to collaboratively develop best practices tailored for DPIA methodologies. Guidance is much needed.

Considering the richness of fundamental rights in the European legal tradition, assessing risks of a processing operation to individuals' rights through DPIAs could be a powerful legal tool to enable what is often described as ethical smart-city development. To account for the plurality and complexity of rights at stake, DPIAs should include multi-perspective risk exploration, and become participatory: Article 35(9) GDPR enables -if not requires- this. Participation in DPIAs is important because rights are not static - their meaning and reasons justifying their limitations are evolving with socio-technological change. Citizens may also perceive risks to their rights differently: in a smart city, one might fear being observed or nudged in public space. Couldn't this amount to a curtailment of privacy, or freedoms of expression and association? Citizens' perceptions are vital to enable municipalities to anticipate and address risks. Citizens involvement can also provide further democratic legitimation for decisions of city officials and councils: such legitimation is particularly important when legal bases and processing purposes are unclear.

Still, municipalities often do not - or are not able to - directly involve citizens in complex discussions about technologies, risks and rights despite the potential of Article 35(9).

They face important challenges. How to operationalise diverse input of those affected by smart-city applications? How to assess concrete risks of an application before its implementation or development? Participation may take additional time and money, and may disturb development processes and the goal to provide innovative solutions. Also, representativeness is as crucial as it is challenging. How to sample a

[18] Project gefinancierd door Research Foundation - Vlaanderen (FWO S006318N). Deze reflectie geeft de visie van de auteurs weer en niet het standpunt van de onderzoekscentra/universiteiten of de financierende organisatie.

group that mirrors the heterogeneity of affected individuals/groups? How to discuss complex topics with groups that have no prior knowledge (or language skills)? And, if participation cannot be representative, is it even useful? We are convinced it is, and note that Article 35(9) also enables the involvement of '*representatives*' of data subjects. Civil society groups, public bodies and entities with mandates to represent certain groups do exist in cities and may represent citizens who may have no interest in being involved. Methods and tools to facilitate public participation are abundant but remain separated from DPIAs due to, e.g., abstract legal provisions, vague guidelines, compliance-oriented controllers, the complexity of technologies. We hope that the DPA's attention in this report will launch efforts to answer the many open questions, as a lot more is still needed to realise participatory DPIAs in (smart) cities: clear guidelines, support and incentives for different actors involved.

Leveraging administrative law

Supporting data protection with administrative law measures could also enhance the protection of citizens' rights. The initiative to register sensors in public spaces is a positive step in this direction. The report rightly notes that it can improve transparency over data processing in the city. But also, it may enable a more strategic risk assessment that could be desirable and necessary to support long-term decision-making. Smart cities are nowadays a patchwork of different projects, and proportionality and risks are examined within the boundaries of specific projects. Little attention is given to possible impacts from the combined effects of the different interventions that slowly aggregate in public space and urban governance (Edwards, 2016, 52-53). Yet, perhaps the most difficult questions concern projects' accumulation. How much privacy loss is acceptable for the urban dweller? At which point could datafication transform the city into an alien environment for digitally illiterate citizens? Administrative law could create participatory processes requiring the mapping and strategic assessment of impacts - inspiration may be drawn from environmental law, which includes processes aimed to assess cumulative impacts. Administrative law could also institutionalize the involvement of democratically-elected city councils, by requiring them to discuss and approve the purchase and use of data processing technologies in smart cities (Galič, 2019, 353).

More attention should also be given to public procurement's role in smart cities. As technologies are designed and deployed by private vendors, the relationship between them and municipalities should ensure that control and accountability for protecting citizens' rights primarily rest with the latter. There are evident links between public procurement and data protection, but operationalizing them is difficult. Procurement is tailored for objectives like open competition and sound procedural management, so inserting participation and fundamental rights considerations in highly bureaucratic processes can be challenging (Mulligan and Bamberger, 2019). Is/should there be space for participation and public hearings during the procurement process? What are the necessary requirements to introduce in tendering documents and contracts to protect citizens' rights? Smart-city tailored data protection standards could possibly facilitate the selection of suitable partners, yet certification and codes of conduct under the GDPR are at their infancy. While procurement could be used strategically for a rights-respectful city, the aforementioned raise pertinent questions that deserve more attention by smart city research and practice.

Recommendations

We would like to conclude with three final recommendations for cities. First, leverage Article 35(9) GDPR. While guidance is still needed and DPAs could have a more active role in (co)developing such guidance, cities could only learn by doing. Second, it is important to educate city councils about the possible challenges of smart cities for fundamental rights, and how these may be addressed, for instance through training and workshops. Increasing council members' digital literacy can lead to better decision-making and more democratic control over smart cities. Third, we recommend cities to increase cooperation between the data protection and procurement departments, e.g. by establishing regular consultations or the co-drafting and -negotiation of contracts.

References

Lilian Edwards, 'Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective, 2 Eur. Data Prot. L. Rev. 28 (2016)

Maša Galič, Surveillance and privacy in smart cities and living labs: Conceptualising privacy for public space. Optima Grafische Communicatie (2019) <https://pure.uvt.nl/ws/portalfiles/portal/31748824/Galic_Surveillance_19_11_2019.pdf>

Deirdre K. Mulligan and Kenneth A. Bamberger, 'Procurement As Policy: Administrative Process for Machine Learning' Berkeley Technology Law Journal, Vol. 34, 2019

6. Grip op de smart city

Digitalisering van de samenleving gaat over meer dan alleen de bescherming van persoonsgegevens, die veelal gericht is op de rechten van het individu. Smart cities vragen ook om aandacht voor maatschappelijke en democratische waarden zoals eigenaarschap van data en grondrechten. Deze waarden raken aan het collectief en de lange termijn-ontwikkelingen en -effecten van smart city-toepassingen. Gegevensbescherming moet daarom niet als losstaand element worden gezien bij digitalisering en smart cities, maar als onderdeel van een groter speelveld waarin andere, soms conflicterende, belangen ook een rol spelen. Het inzetten van technische mogelijkheden dient onderdeel te zijn van een bredere discussie binnen gemeenten waarin deze maatschappelijke en democratische waarden moeten worden betrokken. De AP besteedt daarom in dit onderzoek niet alleen aandacht aan de AVG, maar ook aan beleidsvorming rondom smart cities, ethiek, de rol van de politiek en burgers alsmede sensorregisters.

6.1 Beleid smart cities

De Nederlandse smart city is op een omslagpunt gekomen waarop het van een lappendeken van kleinschalige projecten zou moeten groeien naar een brede visie op de inzet van technologie en data in de openbare ruimte. Het ontwikkelen van beleid rondom digitalisering en smart cities, met de kaders van de AVG, is daarvoor van belang. Door in beleid vast te stellen welke kernprincipes de gemeente hanteert, waaronder over de bescherming van persoonsgegevens, kan zij voor zichzelf kaders scheppen waarbinnen zij dient te handelen in de toekomstige ontwikkeling van smart city-toepassingen in plaats van dat dit per project of ontwikkeling wordt vastgesteld. Door het vaststellen van kaders kan worden voorkomen dat gemaakte keuzes bij verschillende smart city-toepassingen met elkaar conflicteren, iets wat in de praktijk niet zelden voor komt. Bovendien legt zij daarmee verantwoording af aan de burger over de principes/waarden die zij hanteert, waaronder over de bescherming van persoonsgegevens.

Uit het onderzoek blijkt dat vooral de grote gemeenten aangeven over beleidsdocumenten rondom digitalisering/digitale stad te beschikken. Ook wordt regelmatig verwezen naar de ‘Principes voor de digitale samenleving’ van de VNG die is ondertekend door alle gemeenten.[19] Kleinere gemeentes hebben vaak geen specifiek beleid rondom smart cities.

Niet altijd bieden principes en beleid voldoende handvatten voor de praktijk. Doorontwikkeling van deze principes is daarom noodzakelijk om deze effectief toe te kunnen passen. Een voorbeeld betreft het toepassen van privacy by design door gemeenten: van belang is niet alleen *dat* een gemeente dit toepast, maar vooral uitwerkt *hoe* zij dit toepast op zaken als bewaartermijnen, beveiligingstechnologieën (waaronder anonimiseren) en rechten van betrokkenen. We moedigen ‘voortrekkers’ daarom aan om een rol te (blijven) vervullen in het nader uitwerken en delen van kennis op dit vlak, zodat ook kleinere gemeenten hiervan kunnen profiteren.

Aanbeveling: Stel beleid en principes vast rondom smart cities/digitalisering die de kaders van de AVG in acht nemen en werk deze uit in concrete instructies voor de werkvloer. Maak daarbij gebruik van reeds bestaande kennis en ervaringen zodat deze kunnen worden gedeeld met andere gemeenten.

[19] https://vng.nl/artikelen/principes-voor-de-digitale-samenleving

6.2 Ethiek en smart cities

Wet- en regelgeving wordt vaak beschreven als 'gestolde ethiek'. Ethiek kan echter niet vervangen worden door een vastgestelde set van wet- en regelgeving. Dit wordt duidelijk in de gemeenten die door de AP zijn onderzocht. Veel gemeenten geven aan behoefte te hebben aan een ethisch kader dat breder is dan de geldende wet- en regelgeving zoals de AVG, die zich vooral richt op de rechten en vrijheden van het individu. Veelal wordt deze behoefte versterkt door de burgers en gemeenteraad die niet alleen willen weten of nieuwe projecten voldoen aan wettelijke kaders, maar ook de vraag stellen of het juist is om technologie op deze wijze en op deze plek in te zetten. Een deel van deze 'is het juist'-vraag wordt ondervangen door de AVG en de daarin vastgelegde accountabilityverplichtingen. Wanneer deze verplichtingen volledig en serieus worden ingevuld en opgevolgd dan biedt dit houvast om al een belangrijk deel van de ethische vragen te adresseren of ethische afwegingen inzichtelijk te maken. De behoefte aan een uitgebreid ethisch kader is begrijpelijk, bij het verwerken van persoonsgegevens in smart city-projecten dient de gemeente echter te starten met een passende en kwalitatief goede DPIA waarin al een deel van deze vragen worden geadresseerd. Uiteraard kan dit in vervolgstappen worden aangevuld met een ethisch kader dat thema's adresseert die niet in de DPIA aan de orde komen, de AP moedigt dit ook aan. De AVG verlangt op diverse punten ook dat er niet alleen rekenschap wordt gegeven van het recht op gegevensbescherming, maar ook van andere grondrechten.[20]

De AP heeft gezien dat wethouders en gemeenten een dialoog over de ethische vragen over de smart city in de breedte willen voeren. Zo'n brede dialoog is aan te raden. In zo'n brede dialoog met allerlei betrokkenen kunnen vragen aan de orde komen over de technische, juridische, organisatorische en ethische kant van het gebruik van technologie door en binnen een gemeente. Vragen over transparantie richting burgers maar ook over inclusie van burgers bij ontwikkelingen kunnen onderdeel zijn van de te voeren discussie. Dit kan resulteren in een kader of visie van de gemeente inzake digitalisering in het algemeen, en smart cities in het bijzonder. Enkele gemeenten werken al met ethische kaders of een ethische commissie die vroegtijdig betrokken is bij ontwikkelingen op dit vlak. In gemeenten waar dit aanwezig is wordt dit als waardevol gezien en wordt ook de gemeenteraad gezien als een partij waarbinnen vragen over ethiek spelen en besproken zouden moeten worden. De AP vindt dit een positieve ontwikkeling.

Aanbeveling: Ethiek kan niet worden vervangen door vastgestelde wet- en regelgeving. Begin daarom bij het uitvoeren van een DPIA om vraagstukken over gegevensbescherming te adresseren. Voor vragen die de AVG overstijgen kan een ethisch kader worden ontwikkeld en toegepast.

6.3 Een democratische smart city

De openbare ruimte moet ten dienste van de gehele samenleving zijn. De inzet van smart city-toepassingen dient daarom de burger centraal te stellen. Dit vraagt om werkwijzen waarbij burgers worden betrokken, inzicht en een mate van controle wordt gegeven over de technologie en data die in de openbare ruimte wordt verzameld en gebruikt. Smart city-toepassingen lijken in Nederland vooral technologie- en datagedreven te zijn en met name voor gemeentelijke en private belangen te worden gezet, zoals handhaving van de openbare orde en commerciële doeleinden. Slechts in een aantal gevallen zijn smart city-toepassingen van gemeenten gericht op het betrekken van de burgers, het faciliteren van de behoefte van inwoners of het versterken van het democratisch stelsel. Het gevaar bestaat dat *Dataïsme*, het geloof in data als oplossing voor alle problemen, gegevensdeling met oog voor de rechten en vrijheden van

[20] In het kader van de DPIA bepalen de guidelines van de EDPB bijvoorbeeld: "(...) de verwijzing naar "de rechten en vrijheden" van betrokkenen [heeft] voornamelijk betrekking op de rechten op gegevensbescherming en privacy, maar kan ze ook andere grondrechten betreffen zoals vrijheid van meningsuiting, vrijheid van gedachte, vrijheid van verkeer, discriminatieverbod, recht op vrijheid, en vrijheid van geweten en godsdienst."

het individu en daarmee verantwoorde en duurzame innovatie onmogelijk maakt. Om de controle op de inzet van smart city-toepassingen een meer democratische inbedding te krijgen, waarbij burgers (indirect) zeggenschap krijgen, ziet de AP een belangrijke taak weggelegd voor de gemeenteraad en het college, alsmede voor ambtenaren om burgers en inwoners van smart cities te betrekken de inzet en besluitvorming van smart city-toepassingen.

6.3.1 Rol gemeenteraad en college

Gemeenteraden spelen een cruciale rol in de ontwikkeling van, en het debat rondom smart cities. Zo hebben zij uiteraard de taak tot het controleren van het college van B&W. De gemeenteraad is de democratisch gekozen vertegenwoordiging van de burgers in een gemeente en verdient in die rol uitleg, transparantie en de mogelijkheid om het bestuur te controleren. De AP ziet dat de gemeenteraad bij uitstek een belangrijke controlerende rol kan vervullen ten aanzien van smart city- en digitaliseringsaspecten. De gemeenteraad kan bijvoorbeeld vragen stellen over de realisatie van beleidsdoeleinden uit een pilot, de opties voor alternatieve, 'niet technologische' oplossingen en de getroffen waarborgen bij een smart city-toepassing.

We merken op dat smart cities nog niet binnen alle gemeenteraden op het netvlies staan. Digitalisering en de maatschappelijke impact daarvan vormen zelden onderwerp van gesprek.[21] Het gebrek aan kennis bij raadsleden draagt daar niet aan bij. Daar waar gemeenteraden onvoldoende op de hoogte zijn van de specifieke kenmerken van smart cities en de relatie daarvan met de AVG, kunnen ze niet altijd de juiste vragen stellen. Daarnaast kan dit onbedoeld leiden tot moties vanuit gemeenteraden die niet goed zijn uit te voeren omdat ze in strijd lijken te zijn met wet- en regelgeving of een eventueel aanwezig ethisch kader of beleid van de gemeente zelf. Binnen sommige gemeenten zien we wethouders die initiatieven ontplooien om hun gemeenteraad voor te lichten rondom vraagstukken aangaande privacy, ethiek en de meer technische kant van smart cities. Ook is er in een aantal gevallen een goede samenwerking tussen de gemeenteraad en de FG. Dat zijn ontwikkelingen die de AP verwelkomt.

De AP adviseert gemeenteraden en politieke partijen om meer kennis van de digitale wereld op te doen, dat versterkt hun mogelijkheden tot effectieve controle en maakt dat ze goede vragen kunnen stellen bij nieuwe initiatieven. Uiteindelijk vinden daardoor inhoudelijkere discussies plaats hetgeen ten goede komt aan de afwegingen die worden gemaakt rondom smart cities. Een denkraam zoals is opgesteld door het Rathenau Instituut kan een instrument zijn om niet alleen gegevensbescherming, maar ook ethische en maatschappelijke aspecten bespreekbaar te maken binnen de raad.[22] Ook de FG kan in zijn rol als toezichthouder een voorlichtende rol spelen in het informeren van de raad over specifieke knelpunten die raken aan gegevensbescherming. Het college, gemeenteraden en FG´s kunnen ook gebruik maken van de inbreng van burgerrechtenbewegingen, omdat die goed geïnformeerd tegen kunnen denken, zodat met scherpte tijdig en goed nagedacht wordt over de rechten en vrijheden van burgers. Dan worden problemen beter doorzien en kan scherper doorgevraagd worden op voorliggende plannen.

De gemeente dient niet alleen *over* burgers praten, maar ook *met* burgers. Zeker daar waar smart city-toepassingen burgers verdergaand raken in hun rechten is het van belang, en in sommige gevallen zelfs verplicht, hen te betrekken in deze discussie zodat hun perspectief kan worden meegenomen in de ontwikkeling en de risicoanalyse[23]. Zo zou ook de gemeenteraad burgers kunnen (laten) bevragen naar hun mening over een bepaalde smart city-toepassing, mocht de gemeente dat zelf niet al hebben gedaan.

[21] Raad weten met digitalisering, p. 18 e.v.
[22] Raad weten met digitalisering.
[23] Zie ook het onderdeel 'Burgers & oplossingen' verderop in dit rapport.

Aanbeveling: Zorg dat de gemeenteraad meer wordt geïnformeerd over de inzet van en het proces rondom smart city-toepassingen door de gemeente, zodat er meer debat mogelijk is over het onderwerp. Binnen de gemeenteraad moet voldoende kennis geborgd zijn over digitalisering en technologie. Zo nodig kan de gemeenteraad zich laten informeren door deskundigen, zoals de FG, burgerrechtenbewegingen en (gemeentelijke) experts.

Naast de controlerende rol van de gemeenteraad heeft de AP ook gekeken naar de rol van wethouders. In de praktijk zien we dat niet iedere gemeente een wethouder heeft die zich bezighoudt met digitalisering en smart cities. De verantwoordelijke wethouder zal dus verschillen per ingezette toepassing. Dat is op zich niet bezwaarlijk, maar het gevolg kan zijn dat digitalisering en de inzet van smart city-toepassingen vanuit de verschillende domeinen vanuit een verkokerde visie wordt aangepakt, terwijl de effecten domeinoverstijgend zijn. Het kan daarom meerwaarde hebben om een wethouder specifiek verantwoordelijk te maken voor digitalisering. In de gemeenten waar dit het geval is en die de AP heeft gesproken in het kader van dit onderzoek wordt dit ervaren als een positieve invloed op het in goede banen leiden van deze ontwikkeling. Deze wethouder heeft bij voorkeur kennis van het onderwerp en kan helpen om de kaders te bepalen waarbinnen de gemeente handelt bij digitaliseringsvraagstukken, waaronder smart cities. Op die manier heeft de gemeenteraad een (gespecialiseerd) aanspreekpunt en kan deze wethouder het overzicht bepalen en ervoor zorgen dat de gehele gemeentelijke organisatie vanuit dezelfde principes werkt, ook als deze raken aan de 'klassieke' domeinen als milieu, mobiliteit en veiligheid die bij andere wethouders en de burgemeester zijn belegd.

Aanbeveling: Ga de mogelijkheden na om een specifieke wethouder aan te wijzen die zich bezighoudt met digitalisering of bekijk wie er binnen het college kan worden aangesproken over domeinoverstijgende digitaliseringsvraagstukken.

6.3.2 Betrokkenheid burgers

Data vormt slechts een facet van de werkelijkheid. Om werkelijk inzicht te krijgen in de openbare ruimte is het altijd nodig om oog te houden voor de onderliggende culture, politieke en maatschappelijke aspecten. Oplossingen voor bepaalde (maatschappelijke) problemen kunnen en hoeven niet alleen te worden gevonden in data en technologie. Technologie is bovendien niet neutraal; data wordt gegenereerd en weergegeven op basis van keuzes die door mensen zijn gemaakt. Bijvoorbeeld over welke data wordt verzameld, op welke locaties en de wijze waarop data wordt gevisualiseerd. De echte kennis over de openbare ruimte zit bij de gebruikers daarvan: de burger. Daarom is het van belang om bij het bepalen van de wenselijkheid, mogelijkheden en risico's van het verzamelen van data in en over de openbare ruimte het in veel gevallen onontkomelijk om burgers in een vroeg stadium (zoals tijdens het uitvoeren van een DPIA) om hun mening te vragen. Hierbij verdient diversiteit van de groep betrokken burgers speciale aandacht.

Het feit dat burgers vaker niet dan wel betrokken worden bij de besluitvorming en ontwikkeling van smart city-toepassingen hangt mede samen met het feit dat veel smart city-toepassingen een 'top-down'-oplossing zijn, waarbij niet zozeer de burgers, maar de gemeente bepaalt om technologie in te zetten voor bepaalde problemen. Het betrekken van burgers gebeurt dan minder vaak door gemeenten dan wanneer smart city-toepassingen 'bottom-up' (dus meer op initiatief en met invloed van de burger) worden ontwikkeld. Wat opvalt in dit kader is dat projecten die draaien om nieuwe technologie in veel gevallen voorrang krijgen op projecten die transparantie bevorderen of het democratisch proces versterken. Denk hierbij aan projecten die sensoren en data inzichtelijk maken, burgers een rol geven in het proces of

aansluiten bij de democratische structuur. De groei van initiatieven om dit te faciliteren blijft duidelijk achter, terwijl juist deze projecten macht terug bij de burgers kunnen brengen en de stad écht slim maken.

Waar burgers wel worden betrokken door gemeenten is hierin geen eenduidige vorm of aanpak te onderscheiden. Sommige gemeenten geven aan dat burgers al indirect zijn betrokken, namelijk via de verkozen vertegenwoordigers in de gemeenteraad. Geen van de onderzochte gemeenten heeft uitgewerkt in welke gevallen een burger wel of niet wordt betrokken. Dit wordt op ad-hoc basis bepaald. Bekende vormen van betrokkenheid zijn wel genoemd door een aantal gemeenten, zoals burgerpanels, bewonersavonden en voorlichtingsbijeenkomsten. Daarnaast lijken steeds meer gemeenten de mogelijkheden te verkennen naar online burgerparticipatie, waarbij burgers via online kanalen input kunnen geven op (voorgenomen) gemeentelijke ontwikkelingen, al betreft dit meestal andere ontwikkelingen dan specifiek smart city-toepassingen. Over het algemeen lijken gemeenten die burgers betrekken positieve ervaringen te hebben met dit proces doordat smart city-toepassingen meer draagvlak krijgen. Sommige gemeenten geven aan wel burgers te willen betrekken, maar nog worstelen hoe daar praktisch uitvoering aan te geven. Als de burger wordt gevraagd naar zijn mening, dan lijken gemeenten burgers niet altijd te bevragen naar privacyvraagstukken van smart city-toepassingen. Gemeenten die burgers betrekken op privacyvraagstukken geven aan dat representativiteit van de bevraagde groep een punt van aandacht is.

Het is overigens niet altijd nodig om burgers actief te betrekken, bijvoorbeeld als de risico's van bepaalde smart city-toepassingen beperkt zijn. Wanneer in de openbare ruimte persoonsgegevens worden verwerkt is er al snel sprake van grootschaligheid met bijbehorende risico's. Omdat burgers hier geen keuze hebben en het niet altijd kunnen voorzien ligt het betrekken van burgers bij smart city-toepassingen in veel gevallen wel voor de hand. Welke vorm van betrokkenheid het meest passend is, is maatwerk.[24] Wanneer burgers worden gevraagd om hun mening over een voorgenomen verwerking is het interessant om hen niet enkel te bevragen op hun individuele perspectief, maar als vertegenwoordiger van (een deel van) de samenleving. Omdat smart city-toepassingen de openbare ruimte betreffen dient het perspectief van alle groepen meegenomen te worden, ook die van minderheden om de brede samenleving te betrekken bij het ontwikkelen van een smart city.

Aanbeveling: Denk na in welke gevallen, op welk moment en op welke wijze burgers worden betrokken bij de ontwikkeling van smart city-toepassingen. Ga daarbij met name in op de rol van de burger bij het bepalen van de wenselijkheid, mogelijkheden en risico's van het verzamelen van data in en over de openbare ruimte. Ga daarbij expliciet in op het privacy-aspect van smart city-toepassingen.

6.4 Regulering door gemeenten en sensorregisters

Naast gemeenten kunnen ook private partijen sensoren inzetten om (persoons)gegevens in de openbare ruimte te verzamelen. De inzet van gegevensverwerkingen door private partijen in de openbare ruimte is aan strenge eisen gebonden en in veel gevallen verboden. De verwerking van persoonsgegevens in de openbare ruimte valt primair onder de verantwoordelijkheid van, of moet mogelijk zijn gemaakt door, de (wetgevende) overheid. Een private partij zoals een bedrijf heeft daar doorgaans geen gezag.[25]

Een burger zal bij de aanwezigheid van sensoren in de openbare ruimte zich in eerste instantie tot de gemeente richten die de openbare ruimte beheert en controleert. Gemeenten zijn weliswaar niet de

[24] De zogenaamde 'participatieladder' zou ondersteunend kunnen zijn voor de beantwoording van deze vraag.
[25] Dit wil echter niet zeggen dat er nooit persoonsgegevens mogen worden verwerkt in de openbare ruimte door private partijen. Zie ook: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/internet-en-telecom#faq.

verwerkingsverantwoordelijke voor deze sensoren in de zin van de AVG, toch kunnen zij als beheerder van de openbare ruimte niet langs de zijlijn blijven. Zeker niet als de inzet van sensoren indruist tegen gemeentelijk beleid en principes. Op dit moment zien we dat gemeenten de verwerking van persoonsgegevens door private partijen in de openbare ruimte niet goed in kaart hebben. De AP ziet voor gemeenten daarom een taak weggelegd om na te gaan hoe zij grip kunnen krijgen op deze sensoren en andere toepassingen in de openbare ruimte van private partijen waarbij persoonsgegevens worden verwerkt, al dan niet door regulering. Het is van belang voor gemeenten om grip te houden op sensoren in de openbare ruimte om deze, met bijbehorende dataverzameling, te kunnen beheersen en transparantie te kunnen bieden.

Een aantal gemeenten werkt met sensorregisters. In dergelijke (openbare) registers die door de gemeente worden bijgehouden kunnen burgers raadplegen welke sensoren of andere toepassingen (zoals camera's) worden ingezet in de openbare ruimte. Het gaat daarbij niet alleen om sensoren en andere toepassingen van de gemeente, maar ook van private partijen. De AP spreekt haar waardering uit voor deze initiatieven. Een sensorregister kan een instrument zijn om de transparantie vergroten, burgers te betrekken, verantwoording af te leggen, en controle te houden over de ontwikkelingen zowel binnen het publieke als het private domein waar het de openbare ruimte betreft. Tot nu toe vindt het bijhouden van deze registers vooral plaats op basis van vrijwillige medewerking. Gemeenten geven aan dat het hen aan (wettelijke) mogelijkheden ontbreekt om inzicht te krijgen welke sensoren en toepassingen in de openbare ruimte zijn, wie daarvoor verantwoordelijk is en wát deze sensoren exact doen en welke gegevens zij verwerken. De gemeente Amsterdam is voornemens om een meldingsplicht voor sensoren in te voeren in de APV[26] en de gemeente Utrecht heeft een meldplicht om camera's in de openbare ruimte aan te melden[27]. Een eerste stap daartoe kan zijn het invoeren van een register zodat burgers op de hoogte kunnen worden gesteld van sensoren. Al dan niet gekoppeld aan optische kenmerken die sensoren herkenbaar maken.

Een tweede stap zou kunnen zijn om, op termijn, te onderzoeken of het mogelijk en wenselijk is om voorwaarden te verbinden aan de inzet van sensoren en datavergaringen in de openbare ruimte, bijvoorbeeld door middel van een vergunningstelsel. Gemeenten kunnen dan voorwaarden stellen aan private partijen, zoals verplicht gebruik van open source-technologie, eisen aan informatie richting het publiek met bijvoorbeeld duidelijke borden, het enkel opslaan van data in de EU of Nederland, enzovoorts. Het is aan te raden om (in VNG-verband) verder te verkennen of er, bijvoorbeeld in de Gemeentewet, een expliciete mogelijkheid zou moeten komen tot het stellen van regels aangaande het plaatsen van sensoren in de openbare ruimte door private partijen. De vraag blijft overigens of datavergaringen door private partijen zijn toegestaan op grond van de AVG of wenselijk zijn; een dergelijk vergunningenstelsel ontslaat partijen niet om de AVG na te leven. Gemeenten kunnen door het verbinden van voorwaarden wel beter inzicht krijgen in datavergaringen in de openbare ruimte en nadere beperkingen aanbrengen als deze in strijd zijn met de AVG en/of gemeentelijk beleid.

Aanbeveling: Onderzoek op welke wijzen gemeenten inzicht kunnen krijgen in de sensoren die door derden in de openbare ruimte worden geplaatst als deze persoonsgegevens verwerken. Deel informatie over deze sensoren met burgers, zo mogelijk op een centrale locatie zoals door middel van een sensorregister. Denk (samen met andere gemeenten) na over de mogelijkheid en wenselijkheid voor gemeenten om voorwaarden te verbinden voorafgaand aan de inzet van sensoren in de openbare ruimte, zodat burgers zich vrij in de openbare ruimte kunnen blijven bewegen.

[26] https://bekendmakingen.amsterdam.nl/bekendmakingen/publicatie/inspraak/inspraak-sensoren/
[27] https://www.utrecht.nl/bestuur-en-organisatie/privacy/cameras/

7. Reflectie: Voorbij de participatie, zet de burger centraal in slimme stad

Auteur: Judith Veenkamp
Organisatie: Waag
Judith Veenkamp werkt voor Waag, een Future Lab voor technologie en samenleving en leidt het team dat onderzoek doet naar de rol van burgers in innovatie en digitalisering. Van groepen burgers die zelf luchtkwaliteit meten tot patiënten en zorgverleners die hun eigen zorgoplossing ontwerpen.

Met de toeslagenaffaire en de nasleep daarvan nog vers in ons geheugen, zal niemand je meer tegenspreken als je betoogt dat technologie ontwikkeld en gebruikt moet worden op basis van publieke waarden. Hetzelfde geldt voor de technologie in de zogeheten Smart City. De technologie en data die hierin worden gebruikt, zijn middelen om maatschappelijke vraagstukken te adresseren. Niet alleen over het ontwerpen en ontwikkelen van de technologie, maar ook over de context waarin deze toepassingen vervolgens worden gebruikt, woedt momenteel een stevig debat. Het gedachtegoed van Herman Tjeenk Willink met 'Groter denken, kleiner doen'[28] wordt afgestoft en nieuw leven ingeblazen. De roep om een nieuwe bestuurscultuur waarin de positie van de burger in relatie tot de overheid opnieuw vorm krijgt, klinkt steeds luider. Dit blijkt ook uit het 'Adviesrapport Betrokken bij het klimaat' van de adviescommissie Brenninkmeijer en de publicatie van het rapport 'Grote opgaven in een beperkte ruimte' door Planbureau voor de Leefomgeving. waar expliciet aandacht wordt besteed aan de noodzaak om burgers te betrekken. Maar we moeten echt een stap verder zetten: betrek niet alleen burgers, maar zorg ervoor dat burgerinitiatieven **vanuit** de samenleving hun rechtmatige plek krijgen om beleid te beïnvloeden en richting geven aan Smart City toepassingen.

Ondanks dat het publieke debat over technologie in de stad verschuift en de rol van de burger regelmatig wordt benoemd, blijft de reflex van het tech-optimisme sterk, een geloof dat technologie als oplossing ziet, zonder precies te weten waarvoor. Zo verbaasde ik mij over het fanatisme waarmee in het begin van de coronacrisis door de gemeente Rotterdam camera auto's werden ingezet om de 1,5 meter regel te handhaven in de openbare ruimte, zonder goed na te denken of dit middel zijn doel niet voorbijschoot. Er zijn overduidelijk vraagtekens te zetten bij de manier waarop de technologie van een camera-auto bepaalt of de 1,5 meter wel of niet gewaarborgd wordt, maar het is vooral opmerkelijk dat er in een crisissituatie totaal voorbij wordt gegaan aan de mogelijkheid om elkaar aan te spreken op de noodzaak tot afstand houden. Een methode die vele malen menselijker is en direct effect heeft, dan wanneer de camerabeelden vanuit een meldkamer live worden bekeken. Mijns inziens was de proportionaliteit/subsidiariteit hier zoek. Het belang hiervan wordt in dit AP-rapport besproken. Zou er ook op deze maatregel zijn ingezet als bewoners hadden meegedacht over manieren om het naleven van de 1,5 maatregel te stimuleren dan wel te handhaven?

Ook in minder acute crisissituaties, zoals de energietransitie, woningopgave en stikstofcrisis, wordt hoopvol naar innovatie en technologie gekeken. Om me heen zie ik eenzelfde ambtelijke reflex ontstaan rondom het concept van de *digital twin*. De *digital twin* is een digitale weergave van onze leefomgeving die draait op dataverzamelingen en voorspellende modellen. Met een digitale tweeling kun je de impact van bepaalde interventies doorrekenen en simuleren. Ook hier lijkt de verleiding groot om de *digital twin* tot heilige graal te verheffen en lopen doel en middel al snel door elkaar heen. Private partijen zetten samen

[28] Willink, Herman Tjeenk (2018). *Groter denken, kleiner doen.* Amsterdam: Prometheus

met overheden in op de ontwikkeling van dit instrument, feitelijk een dashboard 2.0. Allereerst is het hier goed om te blijven bedenken dat het altijd om een representatie van de werkelijkheid gaat en dus niet de werkelijkheid zelf is. De mensen die de technologie ontwikkelen, vaak werkzaam bij private ondernemingen of de overheid, bepalen welke data er wel en niet wordt meegenomen en schrijven de algoritmen waar de voorspellende modellen op draaien. Ten tweede bestaat er een reëel risico dat de burger ook in deze tech-innovatie uiteindelijk als subject fungeert waar over gepraat wordt, in plaats van met. Zij hebben niet alleen recht om te weten welke data die hen aangaat wordt verzameld, maar zouden ook een gelijkwaardige plek aan tafel moeten hebben wanneer de *Digital Twin* wordt ontwikkeld en toegepast. Daar wordt bepaald welke data er wordt verzameld, gekoppeld en gebruikt en onder welke voorwaarden. Zo kunnen zij meepraten, mee-ontwerpen en mee-besluiten.

Na ruim een decennium aan experimenteren en *piloten* is de Nederlandse slimme stad op een omslagpunt gekomen. Er is behoefte aan een brede visie op de inzet van technologie en data om de openbare ruimte vorm te geven, te onderhouden en te controleren. Een visie waarin technologie de democratie versterkt in plaats van afbrokkelt en er wordt ingezet op *smart citizens* in plaats van *smart cities.* Bewoners zijn per definitie experts met kennis en ervaringen over hun eigen buurt. Door hen vanaf het prille begin van een Smart City toepassing een gelijkwaardige plek aan tafel te geven, kunnen zij een waardevolle rol spelen in het mee-ontwerpen van de technologie en hun kennis en expertise over hun eigen buurt inzetten om de Smart City toepassing naar een hoger, democratischer niveau te tillen. Alleen op die manier is het mogelijk om publieke waarden te verankeren en checks en balances in te bouwen zodat de technologie het democratisch bestel niet schaadt maar juist kan versterken.

Uit dit rapport blijkt dat enkele gemeenten werken aan meer transparantie met openbare sensorregisters en processen waarbij technologische toepassingen in de openbare ruimte door derden moeten worden gemeld bij de gemeente. Toch lijkt er nog veel werk aan de winkel te zijn. Zo is het heel interessant om de verplichte DPIA (Data Protection Impact Assessment) samen met burgers te doen. De DPIA is dan een handvat in het proces om vroegtijdig het gesprek met de bewoner en/of gebruikers te starten over een maatschappelijk vraagstuk en hoe technologie hierin kan ondersteunen. Het is belangrijk dat er een kundige procesbegeleider is om dit in goede banen te leiden en de ruimte voor de burger te creëren en te bewaken. De Functionaris Gegevensbescherming kan hier een belangrijke rol vervullen.

Maar om echt tot een nieuwe bestuurscultuur te komen waar je als overheid en burger samen vraagstukken oppakt en met behulp van technologie de weg voorwaarts uitstippelt, is het nodig om meer ambitie te tonen. Participatie en het “betrekken van burgers” lijken de toverwoorden in overheidsland. Toch gaat het hier vaak over de overheid die de kaders schept voor de burgers om met hen mee te doen. De gemeente bedenkt waar en wanneer input van de burger gewenst is en organiseert een inspraakavond, ontwerpsessie of desnoods een burgerberaad. Hetzelfde geldt voor DPIA’s waar burgers aan tafel zitten. De bewoners worden bedankt, de gemeente trekt zich terug in haar vesting en gaat zitten broeden op beleid, programma's en interventies. Het wordt tijd dat de gemeente ook in de spiegel durft te kijken en haar eigen werkwijze kritisch onder de loep neemt. Laat het eigen systeem meer los en ga de buurten in. Sluit je als gemeente aan bij bestaande burgerinitiatieven waar al veel energie en expertise zit en waar met hart en ziel aan concrete maatschappelijke vraagstukken wordt gewerkt. Daag jezelf uit om dit het startpunt te laten zijn van de ontwikkeling en inzet van technologie in de openbare ruimte. Pas dan ontstaan er echt Smart City toepassingen die in dienst van de samenleving staan.

8. Privacyorganisatie in de gemeente

Het grondrecht op gegevensbescherming laat zich niet vatten in een papieren werkelijkheid, maar moet in de praktijk vorm krijgen. Hiervoor is een robuuste verankering van gegevensbescherming in de gemeentelijke organisatie onontbeerlijk. Een volwassen smart city vraagt dan ook om een volwassen privacyorganisatie. Een gemeente die als betrouwbare en standvastige partij optreedt kan de rechten van burgers optimaal beschermen en gebruik maken van de kansen die er liggen om technologie en data te democratiseren en de macht hierover weer dichter bij de burger te brengen. Daarom besteden we in dit hoofdstuk ook aandacht aan de privacyorganisatie in de gemeente.[29]

8.1 Privacy in de haarvaten

De vormgeving van de privacyorganisatie is afhankelijk van het karakter en de omvang van de gemeente. In verschillende gemeenten is die organisatie nog in opbouw en in verschillende stadia van volwassenheid. Veel gemeenten organiseren nog onvoldoende privacy in de uitvoering van hun werkzaamheden. Er is nog niet altijd onvoldoende aandacht voor de functie en rol van de FG en nog te vaak worden de verplichtingen onder de AVG gezien als een papieren werkelijkheid die in de praktijk weinig effect lijkt te hebben. Privacy moet in de haarvaten van de organisatie zitten, juist bij een publieke organisatie als een gemeente waar veel persoonsgegevens van burgers worden verwerkt.

Het organiseren van privacy vereist dat gemeenten voldoende mensen en middelen vrijmaken. Aan deze voorwaarden voldoen nog lang niet alle gemeenten. Ook goede positionering van de mensen in de organisatie is belangrijk. Zo hebben sommige gemeenten decentraal privacy officers aangesteld. Dat is zinvol omdat decentrale kennis over de praktijk vaak noodzakelijk is om een goede beoordeling te geven over specifieke vraagstukken. Zeker wanneer smart city-toepassingen voortvloeien uit decentrale organisatieonderdelen, zoals verkeer of handhaving.

Daarnaast is het noodzakelijk om het gesprek over het belang van het recht op gegevensbescherming (tijdig) te voeren binnen de organisatie. Te vaak wordt gegevensbescherming gezien als een recht dat in de weg staat aan andere belangen, zoals veiligheid. Dit creëert ten onrechte polarisatie, want het recht op gegevensbescherming is geen absoluut recht dat boven andere rechten gaat, net zo min als dat geldt voor bijvoorbeeld het recht op veiligheid. Het verwijt dat er ‘niks kan door de AVG’ zien we vooral terugkomen als gegevensbescherming niet van het begin af aan is meegewogen in de belangenafweging. Juist door gegevensbeschermingsaspecten in een vroeg stadium te betrekken kan polarisatie worden voorkomen.

Aanbeveling: Stel voldoende mensen en middelen ter beschikking voor het organiseren van privacy binnen de gemeente, zodat gegevensbescherming voldoende aandacht krijgt in de organisatie en tijdig kan worden meegenomen in het proces.

8.2 Functionaris voor Gegevensbescherming (FG)

De AVG stelt het hebben van een FG verplicht voor een gemeente en verbindt aan deze positie een set van taken, onafhankelijkheid en bescherming om diens functie uit te kunnen oefenen. De FG speelt een sleutelrol in de privacyorganisatie binnen een gemeente. De rol en positie van de FG worden meegenomen

[29] De AP heeft in het kader van dit onderzoek niet expliciet uitvraag gedaan naar de privacyorganisatie van gemeenten, maar wel een aantal vragen gesteld in de interviews. De bevindingen uit dit rapport zijn gedaan op basis van signalen van externen en contacten die de AP onderhoudt met betrokkenen, gemeenten en FG’s.

in het toezicht door de AP in het kader van verantwoordelijkheid en accountability. De FG kan niet ontslagen of gestraft worden voor de uitvoering van diens taken. Het behoeden van de gemeente voor misstappen en het beschermen van de burger is een belangrijke taak voor de gemeentelijke FG. Een college dat vertrouwt op de eigen organisatie moet de rol en positie van de FG serieus nemen en voldoende middelen en slagkracht geven om dit te kunnen vervullen.

Een misverstand dat in de praktijk nog veel voorkomt is dat de FG verantwoordelijk wordt gehouden voor het opstellen en naleven van de AVG. Dat is niet het geval: het college van B&W is hiervoor verantwoordelijk. De FG geeft advies over de naleving van de AVG binnen de kaders van de organisatie en de gemeentelijke praktijk. De FG adviseert hoe verwerkingen rechtmatig, behoorlijk en transparant kunnen plaatsvinden volgens de principes van *privacy by design*. Daarom dient de FG tijdig te worden betrokken in de ontwikkeling van toepassingen en beleid. Ook functioneert de FG als interne toezichthouder die op de hoogte is van AVG-gerelateerde ontwikkelingen en door het overzicht mogelijke problemen kan signaleren en bij de verantwoordelijke onder de aandacht kan brengen. De FG dient dus ook toegang tot het bestuur te hebben. Ten tweede ziet de AP het ook nog veel voorkomen dat de FG verantwoordelijk wordt gehouden voor het uitvoeren van DPIA's. Dat is echter niet zijn rol; de FG voorziet van advies. De FG kan ook een belangrijke bron van informatie zijn voor de gemeenteraad in diens besluitvorming.

In de praktijk ziet de AP een wisselend beeld van de gemeentelijke FG. De invulling van deze rol is afhankelijk van de grootte van de gemeente en de bijbehorende aard van werkzaamheden en verwerkingen. Het kan dus zo zijn dat gemeenten waar het aantal verwerkingen beperkt is een juiste invulling van deze functie kan bereiken door een deeltijd invulling. We merken wel op dat het aantal verwerkingen in de gemeentelijke praktijk groeit en veel gemeenten nog moeite hebben om alle verplichtingen van de AVG in de organisatie in te bedden en na te leven. De AP constateert dat de FG's een belangrijke rol spelen in het in goede banen leiden van de ontwikkeling van onder andere smart city-toepassingen, maar hiervoor niet altijd de positie, middelen of zeggenschap krijgen vanuit de gemeentelijke organisatie. De reden hiervoor verschilt van organisaties die nog groeien richting een volwassen organisatie en daardoor de FG niet optimaal benutten of belasten met verkeerde taken, tot gemeenten die de FG niet volwaardig inzetten of een volwaardige invulling van de positie niet goed mogelijk maken. Dit is een belangrijke reden tot zorg voor de AP.[30]

Aanbeveling: Zorg dat de FG zijn of haar functie onafhankelijk en volgens alle eisen kan invullen. De FG is niet verantwoordelijk voor het beleid en dient ook niet als dusdanig in de organisatie gepositioneerd te worden. Toegang tot het bestuur is onontbeerlijk om een juiste invulling van de functie mogelijk te maken. Zorg dat de FG kennis heeft en kan opdoen van processen en de gemeentelijke praktijk om optimaal te kunnen adviseren en toezicht te kunnen houden. De AP heeft aanbevelingen gedaan over de positionering van de FG.[31]

8.3 Samenwerking

Gemeenten hebben een uitdagend en veelomvattend takenpakket. Geen enkele gemeente geeft aan al haar taken volledig zelfstandig te kunnen uitvoeren. Veel gemeenten verzelfstandigen taken, besteden taken uit of werken samen met andere gemeenten in samenwerkingsverbanden. Bij smart cities speelt mee dat technologische ontwikkelingen zeer snel gaan. Het is bijna ondoenlijk voor gemeenten om van alle

[30] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-verzwaart-toezicht-op-gemeente
[31] Zie ook de aanbevelingen van de AP over positionering van de FG: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-publiceert-uitgangspunten-voor-inrichten-sterk-intern-toezicht

technologische ontwikkelingen volledig op de hoogte te zijn en te blijven. Vaak wordt er daarom samengewerkt met andere, ook private partijen die bijvoorbeeld in opdracht van een gemeente een smart city-toepassing ontwikkelen of met kennis- en onderwijsinstellingen, burgers en andere overheidsinstellingen (zoals ministeries, regioverbanden, provincies, politie, etc.). De samenwerking kan veel verschillende vormen aannemen, zoals gemeenschappelijke beleidsvorming over smart cities, kennisuitwisseling en het gezamenlijk ontwikkelen en implementeren van smart city-toepassingen.

Samenwerking en kennisuitwisseling biedt veel kansen. Gemeenten lopen vaak tegen dezelfde vragen aan in het kader van smart city-toepassingen. Bijvoorbeeld bij het beantwoorden van juridische vraagstukken (bijvoorbeeld over de grondslag, risico's), beleidsmatige vragen (bijvoorbeeld welke smart city-toepassingen al dan niet effectief zijn voor de aanpak van een bepaald probleem en op welke wijze burgers kunnen worden betrokken) en uitvoeringsvraagstukken (bijvoorbeeld bij het formuleren van inkoopvoorwaarden). Daarnaast zouden bijvoorbeeld gezamenlijke inkooptrajecten kunnen helpen om een stevigere positie aan te nemen ten aanzien van invloedrijke marktpartijen. Met name kleinere gemeenten die minder middelen hebben kunnen veel baat hebben bij ondersteuning vanuit andere, grotere gemeenten, kennisorganisaties of koepelorganisaties zoals de VNG. De AP juicht deze vormen van samenwerking toe.

Samen werken aan de ontwikkeling van smart cities mag echter niet omslaan in onachtzaamheid. De gemeente is en blijft, ook in een samenwerkingsrelatie, verantwoordelijk voor de smart city-toepassingen die zij inzet. Gemeenten moeten daarom altijd voldoende kritisch reflecteren op de gepropageerde oplossingen die smart city-toepassingen bieden om na te gaan of deze passend zijn voor de desbetreffende gemeente. Een smart city-toepassing in de ene gemeente hoeft immers niet per definitie succesvol te zijn in de andere gemeente als deze niet aansluit op de specifieke doelen en problematiek in de gemeente. Dit kan zelfs in strijd zijn met de AVG (zie ook het hoofdstuk 'Doelbinding en noodzakelijkheid'). Het is daarom essentieel dat gemeenten blijven denken vanuit het probleem waar de toepassing aan zou moeten bijdragen en niet vanuit de geboden oplossing.

Een gebrek aan kritische reflectie binnen de gemeentelijke organisaties zien we bijvoorbeeld bij aanbestedingen of de uitgifte van vergunningen. Het enkel aangeven dat een opdrachtnemer moet voldoen aan wet- en regelgeving, en dus aan de AVG, is natuurlijk mooi, maar gegeven de specifieke activiteiten passen soms additionele maatregelen. Zeker wanneer de opdrachtnemer gegevens gaat verwerken namens de gemeente vergt de AVG additionele eisen. Gemeenten doen er daarom goed aan zowel bij aanbestedingen en vergunningen diepgaandere eisen te stellen en waarborgen op te nemen. We illustreren dat aan de hand van een in het kader van smart cities veelgenoemde ontwikkeling, te weten *Mobility as a Service* (MaaS) in het volgende hoofdstuk.

Aanbeveling: Zoek de samenwerking op voor de aanpak van gemeenschappelijke vraagstukken rondom smart cities. Laat 'voortrekkers' een leidende rol hierin nemen. Blijf tegelijkertijd kritisch tegenover de inzet van smart city-toepassingen, ook als deze breed worden gedeeld en toegepast; een smart city-toepassing in de ene gemeente hoeft niet per definitie succesvol te zijn in de andere gemeente als deze niet aansluit op de specifieke doelen en problematiek in de gemeente.

9. Ontwikkeling in de praktijk: MaaS

Verkeer en mobiliteit binnen en rondom een gemeente zijn belangrijke aandachtspunten van gemeenten wat zich vertaalt in projecten die bij veel gemeenten als smart city-toepassingen worden getypeerd. Gemeenten zijn individueel en in samenwerkingsverbanden op zoek naar mogelijkheden om mobiliteit duurzamer te maken, capaciteit beter te benutten, maar ook voldoende flexibel te laten zijn om aan te sluiten bij de behoeften van de inwoners. Deze mobiliteitsprojecten vallen onder de term *Mobility as a Service* (MaaS). Om dit in te vullen worden mobiliteitsdiensten gebruikt die middels een platform worden aangeboden. Deze diensten zijn zeer divers en proberen in te spelen op de behoefte van de afnemer, denk aan een te reserveren deelvoertuig, of een app die meerdere soorten vervoer als één pakket aanbiedt. Daarnaast bestaat er de wens om steden niet vol te bouwen met wegen en parkeervoorzieningen. Logischerwijs wordt daarbij ook onderzoek gedaan naar de inzet van digitale middelen. MaaS wordt door veel gemeenten dan ook onderzocht omdat daardoor vervoersmiddelen optimaler kunnen worden gebruikt. MaaS kent veelal meerdere partijen die participeren. Voor vervoersvragen over grotere afstanden tussen gemeenten is in deze projecten vaak data nodig om vraag en aanbod op elkaar af te stemmen. Zeker indien de vervoersvraag niet door één aanbieder kan worden ingevuld, maar bijvoorbeeld door een combinatie van bus, tram en of trein. Daarnaast zijn gemeenten, vaak verenigd in regioverband, verantwoordelijk voor concessies inzake het openbare vervoer in die regio. Data die concessienemers inzake vervoersbewegingen vergaren kan dus nuttig zijn bij MaaS. Gemeenten vervullen daarnaast vaak een rol door het uitgeven van vergunningen aan aanbieders van deelvervoer zoals deelscooters en deelfietsen. Vervoersbewegingen van personen zijn in hoge mate bruikbaar om personen mee te identificeren. Verkeerd gebruik daarvan brengt dus risico's voor de bescherming van persoonsgegevens met zich mee.

Het is daarom aan te raden om bij het afgeven van een vergunning expliciet te letten of en op welke wijze een MaaS aanbieder persoonsgegevens verwerkt, door bijvoorbeeld de accountabilitydocumentatie van een aanbieder te beoordelen. Daar waar een aanbieder bijvoorbeeld onduidelijk is over het doel van en de noodzaak van verwerkingen in een privacyverklaring, onvoldoende bereikbaar is voor betrokkenen, een onduidelijke privacyverklaring heeft of geen maatregelen heeft getroffen om invulling te geven aan het recht van verwijdering, zou een gemeente dit moeten meewegen bij de beslissing tot het afgeven van een vergunning. Naast bijvoorbeeld fysieke veiligheid van de gebruikers van deze diensten zou ook de bescherming van persoonsgegevens van gebruikers een belangrijk element moeten zijn in de beoordeling.

Ook ten aanzien van concessies en aanbestedingen zijn eisen aan de bescherming van persoonsgegevens noodzakelijk. Binnen deze trajecten worden soms eisen gesteld aan het uitwisselen van gegevens tussen partijen. Soms wordt er ook informatie uitgewisseld met de gemeente zelf. Die eisen worden soms ingevuld door te verwijzen naar veelgebruikte industriestandaarden. Standaarden die zijn overgekomen van buiten de EU of die minder recent zijn, zijn niet altijd de meest privacyvriendelijke. Dit terwijl de AVG oplossingen vereist die voldoen aan de eisen van privacy by design. Onvoldoende aandacht voor deze aspecten kan resulteren in bovenmatige verwerking van persoonsgegevens en is daarmee dus in strijd met de AVG. Ook hier is een kritische analyse dus wenselijk.

Gemeenten sporen soms burgers aan om technologie te gebruiken of te installeren, al dan niet met subsidie door de gemeente. Dit werpt vragen op betreffende gegevensbescherming. We noemen hier slechts één aspect, namelijk de vraag of gemeenten bij het bepalen van de keuze van een leverancier hebben stilgestaan bij de vraag of de door het product of de dienst verwerkte persoonsgegevens in de basis

wel voldoet aan de in Europa geldende wet- en regelgeving. In de gevoerde gesprekken gaf één gemeente aan een basischeck op de verwerking van persoonsgegevens uit te voeren alvorens een relatie met die partij aan te gaan of de diensten van die partij binnen de gemeente toe te laten of te promoten.

Hierbij dient ook te worden stilgestaan bij de vraag in hoeverre gemaakte afspraken of gestelde voorwaarden bij vergunningen of aanbestedingen nog steeds actueel en relevant zijn. Techniek en bijbehorende risico's staan niet stil. Vergunningen en aanbestedingen gelden vaak voor langere duur, bij de periodieke evaluatie van de gemaakte afspraken dient ook te worden stilgestaan bij de vraag of de afspraken nog voldoen aan de AVG.

Aanbeveling: Neem bij het opstellen van het programma van eisen bij een aanbesteding, of de voorwaarden die gelden bij een vergunning, expliciet eisen op ten aanzien van de verwerking van persoonsgegevens. Stel periodiek vast of er aan de overeengekomen eisen wordt voldaan, en of de eisen zelf nog in lijn zijn met de AVG.

10. Aanbevelingen

10.1 Basisbeginselen AVG voor de smart city

- Bepaal voordat je aan enige smart city-toepassing begint of er persoonsgegevens worden verwerkt en of de verwerking van persoonsgegevens rechtmatig is. Zonder rechtmatige gegevensverwerking kunnen smart city-toepassingen niet ontwikkeld of toegepast worden.
- Stel vast aan welk(e) doel(en) de smart city-toepassing moet bijdragen. Maak deze doelstellingen zo concreet en meet-/toetsbaar mogelijk om de effectiviteit van de smart city-toepassing vast te stellen. Algemene doeleinden als 'veiligheid' of 'leefbaarheid' moeten nader worden ingevuld. Stel ook vast wat de vervolgstappen zijn als een smart city-toepassing niet slaagt of er ongewenste neveneffecten optreden.
- Ga voorafgaand aan de inzet van smart city-toepassingen na of er alternatieve oplossingen zijn om het doel te bereiken waarbij geen of minder persoonsgegevens worden verwerkt. Denk na vanuit het probleem en niet vanuit de geboden oplossing.

10.2 DPIA's

- Houd DPIA's actueel om de huidige risico's van de verwerking te kunnen aantonen. Openstaande actiepunten in een verouderde DPIA of het niet documenteren van technische aanpassingen in de verwerking voldoen niet aan de verantwoordingsplicht. Bepaal beleid waarbij DPIA's periodiek worden herzien c.q. bijgewerkt.
- Stel het uitvoeren een DPIA niet uit, maar doe dit zo vroeg mogelijk bij de ontwikkeling van smart city-toepassingen. Zeker bij geplande evenementen of andere toepassingen met deadlines is dat van groot belang. Zo kan tijdig worden bepaald of een verwerking eventueel voor voorafgaande raadpleging moet worden ingediend bij de AP. Betrek de FG zo vroeg mogelijk, zodat deze tijdig kan voorzien van advies.
- Publiceer zoveel mogelijk de DPIA's van smart city-toepassingen en ontwikkel beleid over de publicatie van DPIA's.
- Besteed in de DPIA aandacht aan de vraag of betrokkenen naar hun mening is gevraagd en op welke manier er opvolging is gegeven aan deze meningen. Hoe hoger de mogelijke risico's, hoe onduidelijker de wettelijke grondslag of hoe hoger de mate van ervaren inbreuk, hoe meer het voor de hand ligt burgers te betrekken.
- Smart city-toepassingen die zich in de pilotfase bevinden moeten ook voldoen aan de eisen van de AVG indien daarbij persoonsgegevens worden verwerkt. Ga daarom ook bij pilot- en proefprojecten na in hoeverre deze projecten AVG-compliant zijn en voer zo nodig een DPIA uit.
- Wees kritisch bij het beoordelen van de anonimiteit van de gegevens die worden verwerkt; gegevens kunnen pas worden beschouwd als anoniem als voor welke partij dan ook, met inzet van (voor het doel) redelijke middelen, het onwaarschijnlijk is hieruit personen te identificeren.
- Stel bij samenwerkingsverbanden voorafgaand aan de start van de verwerking vast wie waarvoor verwerkingsverantwoordelijk dan wel verwerker is. Wees daarover ook transparant naar burgers.

10.3 Grip op de smart city

- Stel beleid en principes vast rondom smart cities/digitalisering die de kaders van de AVG in acht nemen en werk deze uit in concrete instructies voor de werkvloer. Maak daarbij gebruik van reeds bestaande kennis en ervaringen zodat deze kunnen worden gedeeld met andere gemeenten.

- Ethiek kan niet worden vervangen door vastgestelde wet- en regelgeving. Begin daarom bij het uitvoeren van een DPIA om vraagstukken over gegevensbescherming te adresseren. Voor vragen die de AVG overstijgen kan een ethisch kader worden ontwikkeld en toegepast.
- Zorg dat de gemeenteraad meer wordt geïnformeerd over de inzet van en het proces rondom smart city-toepassingen door de gemeente, zodat er meer debat mogelijk is over het onderwerp. Binnen de gemeenteraad moet voldoende kennis geborgd zijn over digitalisering en technologie. Zo nodig kan de gemeenteraad zich laten informeren door deskundigen, zoals de FG, burgerrechtenbewegingen en (gemeentelijke) experts.
- Ga de mogelijkheden na om een specifieke wethouder aan te wijzen die zich bezighoudt met digitalisering of bekijk wie er binnen het college kan worden aangesproken over domeinoverstijgende digitaliseringsvraagstukken.
- Denk na in welke gevallen, op welk moment en op welke wijze burgers worden betrokken bij de ontwikkeling van smart city-toepassingen. Ga daarbij met name in op de rol van de burger bij het bepalen van de wenselijkheid, mogelijkheden en risico's van het verzamelen van data in en over de openbare ruimte. Ga daarbij expliciet in op het privacy-aspect van smart city-toepassingen.
- Onderzoek op welke wijzen gemeenten inzicht kunnen krijgen in de sensoren die door derden in de openbare ruimte worden geplaatst als deze persoonsgegevens verwerken. Deel informatie over deze sensoren met burgers, zo mogelijk op een centrale locatie zoals door middel van een sensorregister. Denk (samen met andere gemeenten) na over de mogelijkheid en wenselijkheid voor gemeenten om voorwaarden te verbinden voorafgaand aan de inzet van sensoren in de openbare ruimte, zodat burgers zich vrij in de openbare ruimte kunnen blijven bewegen.

10.4 Privacyorganisatie in de gemeente

- Stel voldoende mensen en middelen ter beschikking voor het organiseren van privacy binnen de gemeente, zodat gegevensbescherming voldoende aandacht krijgt in de organisatie en tijdig kan worden meegenomen in het proces.
- Zorg dat de FG zijn of haar functie onafhankelijk en volgens alle eisen kan invullen. De FG is niet verantwoordelijk voor het beleid en dient ook niet als dusdanig in de organisatie gepositioneerd te worden. Toegang tot het bestuur is onontbeerlijk om een juiste invulling van de functie mogelijk te maken. Zorg dat de FG kennis heeft en kan opdoen van processen en de gemeentelijke praktijk om optimaal te kunnen adviseren en toezicht te kunnen houden. De AP heeft aanbevelingen gedaan over de positionering van de FG.[32]
- Zoek de samenwerking op voor de aanpak van gemeenschappelijke vraagstukken rondom smart cities. Laat 'voortrekkers' een leidende rol hierin nemen. Blijf tegelijkertijd kritisch tegenover de inzet van smart city-toepassingen, ook als deze breed worden gedeeld en toegepast; een smart city-toepassing in de ene gemeente hoeft niet per definitie succesvol te zijn in de andere gemeente als deze niet aansluit op de specifieke doelen en problematiek in de gemeente.

10.5 Mobility as a Service (MaaS)

- Neem bij het opstellen van het programma van eisen bij de aanbesteding, of de voorwaarden die gelden bij een vergunning, expliciet eisen op ten aanzien van de verwerking van persoonsgegevens. Stel periodiek vast of er aan de overeengekomen eisen wordt voldaan, en of de eisen zelf nog in lijn zijn met de AVG. Bepaal ook of er sprake is van een relatie waarbinnen een partij verwerker is.

[32] Zie ook de aanbevelingen van de AP over positionering van de FG: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-publiceert-uitgangspunten-voor-inrichten-sterk-intern-toezicht

11. Bijlage: begripsbepalingen

Smart city-toepassing
Het verzamelen en verwerken van (persoons)gegevens over of in de openbare ruimte door de inzet van sensoren, technologie of andere toepassingen om inzicht in, of analysemogelijkheden over de openbare ruimte te verkrijgen, of sturing van de openbare ruimte mogelijk te maken. Bijvoorbeeld wifi- en bluetoothtracking, inzet van (mobiele of gedragen) camera's, of sensoren die data verzamelen over verkeerstoepassingen of geluid.

AVG
In de Algemene verordening gegevensbescherming (AVG) zijn de belangrijkste regels voor de omgang met persoonsgegevens in Nederland vastgelegd. Voorheen was dat in de Wet bescherming persoonsgegevens (Wbp). Vanaf 25 mei 2018 is de AVG van toepassing. Dat betekent dat er sinds die datum dezelfde privacywetgeving geldt in de hele Europese Unie.

UAVG
De AVG is rechtstreeks van toepassing in Nederland. Daar waar de AVG ruimte laat voor nationale keuzes bij de uitvoering van de AVG, zijn deze ingevuld in de Uitvoeringswet AVG (UAVG).

Persoonsgegevens
De Algemene verordening gegevensbescherming (AVG) geeft aan dat een persoonsgegeven alle informatie is over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is.

Verwerking van persoonsgegevens
Indien persoonsgegevens worden verwerkt is er bijvoorbeeld sprake van het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, combineren, afschermen, wissen of vernietigen van gegevens.

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. In de gemeentelijke praktijk is het college van burgemeester en wethouders verwerkingsverantwoordelijke onder de AVG. In specifieke gevallen waarbij het gaat om veiligheidssituaties kan het ook zijn dat de Burgemeester verwerkingsverantwoordelijke is.

Verwerker
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Functionaris gegevensbescherming (FG)
De functionaris gegevensbescherming (FG) is de onafhankelijke interne toezichthouder op AVG-compliance van de verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke is verantwoordelijk voor het opstellen en het uitvoeren van het privacybeleid. De FG ziet toe op de naleving hiervan en brengt advies uit over de risico's van bestaande verwerkingen en nieuwe producten en diensten. De FG ziet er

tevens op toe dat de rechten van betrokkenen effectief kunnen worden uitgeoefend. De FG kan advies verstrekken op de DPIA en treedt op als contactpersoon voor de toezichthoudende autoriteit. De gemeente moet de FG middelen en toegang tot alle informatie en bestuurders verschaffen. De FG mag geen instructies ontvangen of gestraft of ontslagen worden voor de uitoefening van diens taken.

DPIA
Onder de Algemene verordening gegevensbescherming (AVG) kunnen organisaties verplicht zijn een data protection impact assessment (DPIA) uit te voeren. Dat is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En om daarna maatregelen te kunnen nemen om de risico's te verkleinen.

Voorafgaande raadpleging
Indien uit een DPIA naar voren komt dat een beoogde verwerking een hoog risico oplevert en er onvoldoende maatregelen getroffen kunnen worden om het risico te beperken, moet met de Autoriteit Persoonsgegevens (AP) overlegd worden voordat met de verwerking wordt gestart. Dit wordt een voorafgaande raadpleging genoemd. Bij een voorafgaande raadpleging geeft de AP advies hoe de risico's van uw voorgenomen verwerking kunnen worden beperkt. Als deze maatregelen worden uitgevoerd, mag met de verwerking worden begonnen. Het kan ook dat de AP adviseert om helemaal van de verwerking af te zien.

MaaS
Mobility as a Service (MaaS) zijn mobiliteitsservices die middels een (digitaal) platform worden aangeboden. Denk aan deelvoertuigen die via een smartphoneapp kunnen worden gereserveerd, maar ook digitale platformen waarop meerdere soorten vervoer als één pakket worden aangeboden vallen onder MaaS.

Accountability
Onder de AVG moet een gemeente verantwoording kunnen afleggen voor de verwerkingen van persoonsgegevens. Hiervoor dient de gemeente een reeks verplichtingen na te komen om dit mogelijk te maken, de accountabilityverplichtingen. Voorbeelden hiervan zijn het register van verwerkingen, de DPIA en het transparant zijn over verwerkingen van persoonsgegevens.

EDPB
De AP is lid van de European Data Protection Board (EDPB). Dit is een onafhankelijk orgaan waarin alle nationale privacytoezichthouders uit de EU samenwerken. De EDPB zorgt ervoor dat de privacywetgeving consequent wordt toegepast in de EU. Bijvoorbeeld door adviezen, besluiten en guidelines met uitleg over de AVG te publiceren.

12. Bijlage: vragenlijst gemeenten

1. Overzicht smart city-toepassingen

Ten eerste verzoeken wij u een overzicht te geven van alle smart city-toepassingen van na 1 januari 2015, met in het bijzonder de smart city-toepassingen waarbij uw gemeente persoonsgegevens verwerkt en optreedt als verwerkingsverantwoordelijke. Wij willen u vragen om in uw overzicht in ieder geval de volgende gegevens aan te leveren ten aanzien van de smart city-toepassingen:

- Naam van de toepassing;
- Startdatum;
- Einddatum (indien van toepassing);
- Onderwerp (b.v. mobiliteit, veiligheid, etc.);
- Omschrijving van de toepassing, met daarin in ieder geval op hoofdlijnen een omschrijving van:
    - Het doel van de toepassing;
    - De verwerkte (persoons)gegevens;
    - (Technische) informatie over de ingezette middelen voor verkrijging en verwerking van de gegevens.
- DPIA uitgevoerd ja/nee (indien ja: graag meesturen).

2. Vragenlijst

Daarnaast verzoeken wij u de volgende vragen te beantwoorden:

1. Op welk moment betrekt u uw functionaris voor gegevensbescherming (FG) bij de ontwikkeling en inzet van smart city-toepassingen?
2. In hoeverre betrekt u ethische vragen en dilemma's bij uw smart city-toepassingen?
3. Heeft uw gemeente specifiek beleid op smart city-toepassingen? (Indien ja: graag meesturen)
4. Zijn er andere partijen zoals kenniscentra, bewonersgroeperingen, expertgroepen, etc. betrokken bij de ontwikkeling van smart city-toepassingen? Zo ja, welke zijn dat, en welke rol hebben deze partijen gespeeld?
5. Bent u bekend met andere smart city-toepassingen in uw gemeente waarvoor u niet de (enige) verwerkingsverantwoordelijke bent? Kunt u hier voorbeelden van geven en aangeven wie (nog meer) verwerkingsverantwoordelijke is bij deze toepassingen?
6. Zijn er smart city-toepassingen waarbij u samenwerkt met andere gemeenten? Zo ja, om welke vorm van samenwerking gaat het?
7. Heeft uw gemeente in de rol van wetgever de inzet van sensoren, camera's of andere technologische dataverzamelmethoden in de openbare ruimte gereguleerd of heeft u plannen daarvoor?

3. DPIA's

Ten slotte verzoeken wij u om ten aanzien van de smart city-toepassingen van na 1 januari 2015 waarbij uw gemeente optreedt als verwerkingsverantwoordelijke en waarvoor een DPIA verplicht is, de DPIA('s) toe te sturen. Eventuele persoonsgegevens in de DPIA('s) kunt u verwijderen.

13. Slotwoord

Technologie raakt vervlochten in onze steden, en daarmee in onze levens. De AP hoopt met dit rapport een holistische benadering van de Nederlandse smart city met aandacht voor de AVG te stimuleren. Dit rapport kan niet alle vragen beantwoorden, dat is de taak van de verwerkingsverantwoordelijke, maar geeft wel houvast in de zoektocht naar verantwoorde innovatie in de openbare ruimte. Waar er veel zorgen zijn over het kennisniveau en de aandacht voor gegevensbescherming, zijn er ook lichtpuntjes waar het wel de goede kant op gaat. Hier wordt gegevensbescherming vaak ook als uitdaging gezien door ontwikkelaars, wat past in onze Nederlandse kenniseconomie. We roepen gemeenten daarom op verantwoording te nemen en binnen de kaders toepassingen te ontwikkelen. Daarbij moet ook ruimte zijn om na te denken over de wenselijkheid en betekenis van smart city-toepassingen in de maatschappij. En de durf om soms iets niet te doen. Dit is een ingewikkelde opgave, maar resulteert uiteindelijk in duurzame innovatie die de openbare ruimte voor alle burgers verbetert zonder dat burgers daarvoor grondrechten hoeven in te leveren. Hierbij is het van belang om burgers te betrekken bij de ontwikkeling, deze beschikken over onmisbare kennis over hun leefomgeving die bij kan dragen aan duurzame ontwikkeling van de openbare ruimte. We hopen dat dit rapport leidt tot een constructieve dialoog over de toepassing van technologie en data in onze openbare ruimte. De reflecties in dit rapport zijn een eerste aanzet daartoe. Wij bedanken de schrijvers voor hun onafhankelijke reflectie en bijdrage aan het gesprek over duurzame ontwikkeling van de Nederlandse smart city.

Namens de onderzoekers:

- Anna Maj Drenth
- Gerald Hopster
- Arjan Kapteijn
- Celina Romijn
- Maxine Moleman
- Krijn Wijnands

Vragen over de Algemene verordening gegevensbescherming

Op onze website autoriteitpersoonsgegevens.nl vindt u informatie en antwoorden op vragen over de Algemene verordening gegevensbescherming (AVG). Heeft u op deze website geen antwoord op uw vraag gevonden? Dan kunt u contact opnemen met het Informatie- en Meldpunt Privacy van de Autoriteit Persoonsgegevens op 088-1805 250.