Bijlage 3- SCH-AGH Dataprincipes, informatiebeveiliging en AVG

Versie:	Def
Documentdatum:	05 november 2019
Documentnummer:	SCH-AGH Dataprincipes informatiebeveiliging en AVG

SCH-AGH Dataprincipes, informatiebeveiliging en AVG

Doelstelling

De gemeente Hilversum en het consortium hanteren een aantal basisbeginselen bij het gebruik van data in het kader van het Smart City Platform. Deze basisbeginselen zijn gebaseerd op, en vormen een uitwerking van de 'Declaration of Cities Coalition for Digital Rights'.

Omdat de doelstelling en de principes vooral het terrein raken van de eigenaren en de verwerkers van de data, worden deze twee begrippen nader toegelicht.

Eigenaren van de data:

Binnen de context van het SCP is het volgende uitgangspunt leidend voor de eigenaarschap van data:

- De producent van data blijft de eigenaar.

Om dit specifiek te maken:

- Data uit de openbare ruimte zijn van Gemeente Hilversum
- Data geïmporteerd vanuit andere bronnen zijn van deze andere bron.
- Data gemaakt door het verrijken van andere data zijn van de verrijker.

Verwerker van de data:

Het consortium of een andere partij is de verwerker van de data en het consortium voert databeheer uit binnen de richtlijnen van de verwerkersovereenkomst met de gemeente Hilversum, voor zover het de door de gemeente verstrekte data betreft, en met de andere partners zoals dat per usecase beschreven is in de verwerkersovereenkomst.

5 Dataprincipes

Toegankelijk

1. De data die in de openbare ruimte worden verzameld, moeten in beginsel voor eenieder toegankelijk zijn. Dat betekent in ieder geval het volgende:

1.1. Data uit de openbare ruimte verkregen door of in opdracht van de gemeente zijn in principe openbaar, tenzij deze herleidbaar zijn tot een persoon

1.2. Ook private partijen kunnen toestemming krijgen om data te vergaren in de openbare ruimte. We streven ernaar dat ook deze data voor eenieder toegankelijk zijn, maar erkennen mogelijke commerciële belangen. In deze gevallen kan het dus zijn dat een redelijke vergoeding voor deze data wordt gevraagd.

1.3. Voor data die een commercieel belang vertegenwoordigen en data die wat vertrouwelijkheid betreft aan richtlijnen onderhevig is kunnen beperkingen ten aanzien van de toegankelijkheid worden opgelegd.

Transparant

2. Iedereen moet toegang hebben tot heldere informatie over de datasystemen in de openbare ruimte (zoals techniek, algoritmes en artificial intelligence) en daarmee de mogelijkheid hebben om eventuele schending van de dataprincipes aan de orde te stellen. Dit betekent onder meer het volgende:

2.1. De gemeente heeft de regie over data die in de openbare ruimte worden verzameld. Hiervoor wordt binnen het Smart City Platform een data- en sensorregister ingericht. Het sensorregister biedt inzicht in welke data in de openbare ruimte worden verzameld, onafhankelijk of de data wel of niet opengesteld kunnen worden.

2.2. Van sensoren worden o.a. de locatie, eigenaar, type sensor, sensor unieke identificatiecode, versie van de software op de sensor en type verzamelde data vastgelegd in een sensorregister. Private partijen krijgen toestemming om gegevens te verzamelen in de openbare ruimte op voorwaarde dat ze deze registratie in het sensorregister doen en bij wijzigingen van de sensorattributen in het register deze doorgeven aan de beheerder van het register.

2.3. Het sensorregister is openbaar toegankelijk en kan vrij door eenieder worden geraadpleegd.

2.4. Van alle data die op het platform worden vastgelegd worden de belangrijkste attributen zoals verwerkingsverantwoordelijke en verwerker van alle data, data-elementen en de relatie naar het sensorregister, het verwerkingsregister en de referenties naar de Data Privacy Impact Assessments (DPIA) en de verwerkersovereenkomsten bijgehouden.

Veilig

3. Iedereen heeft recht op de bescherming van zijn eigen persoonsgegevens en het recht om te weten en te bepalen wat er met zijn eigen persoonsgegevens gebeurt. Voor het Smart City Platform wordt dit beginsel minimaal als volgt vertaald:

3.1. In het ontwerp van het Smart City Platform geldt privacy by design als uitgangspunt.

3.2. Voor zover verzamelen van persoonsgegevens onvermijdelijk of noodzakelijk is, wordt strikt erop toegezien dat de regels van de Algemene Verordening Gegevensbescherming worden nageleefd.

3.3. In ieder geval worden gegevens pas opengesteld nadat ze zodanig zijn verwerkt (bijvoorbeeld geanonimiseerd of geaggregeerd) dat de privacy risico's gedekt zijn. Dit geldt zowel voor data die zijn verzameld door de gemeente als door private partijen.

3.4. Het is niet toegestaan om geanonimiseerde gegevens die afkomstig zijn van het platform door het gebruik van aanvullende gegevens weer aan een natuurlijke persoon te koppelen.

3.5. Alle onderdelen van het Smart City Platform voldoen tenminste aan actuele normen voor overheidsdiensten en wetgeving op het gebied van gegevensbeveiliging en toegang.

3.6. Bij het verzamelen van data in de openbare ruimte streeft de gemeente naar een goede kwaliteit van data. Op de kwaliteit van de data die door private partijen worden verzameld kan de gemeente geen invloed uitoefenen, maar wel randvoorwaarden voorschrijven. De gemeente maakt afspraken met de private partijen over juist gebruik van data. De gemeente is niet aansprakelijk voor het onjuist gebruik van data door derden.

Open

4. Uitgangspunt is dat eenieder op een gelijkwaardige wijze toegang heeft tot dezelfde data en onder dezelfde voorwaarden data mag verzamelen en/of publiceren op het Smart City Platform.

4.1. Voor de data die zijn verzameld door of in opdracht van de gemeente geldt dat er geen technische of juridische belemmeringen worden opgeworpen die toegang tot open data onmogelijk maken, beperken of discrimineren.

4.2. Voor de data die zijn verzameld door of in opdracht van private partijen geldt dat mogelijk een vergoeding moet worden betaald in ruil voor verkrijging of bewerking van de data.

4.3. Iedereen moet in staat zijn om eigen technologie te gebruiken. Voor het Smart City Platform is het uitgangspunt dat het platform met alle beschikbare oplossingen werkt, zodanig dat anderen het op gelijke wijze in de eigen digitale dienstverlening en of toepassing kunnen gebruiken.

Kwaliteit

5. Uitgangspunt is dat de data die beschikbaar wordt gesteld van een vastgesteld kwalitatief niveau is, zodat (potentiele) gebruikers van de data kunnen vaststellen of dit voldoende is voor het doel waarvoor zij de data willen gebruiken. Voor het Smart City Platform wordt dit beginsel minimaal als volgt vertaald:

5.1. De kwaliteit van de data die opgenomen worden op het platform dient vastgelegd te zijn. Dat wil zeggen dat vanuit de doelbinding voor de data beschreven moet zijn wat de kwaliteitseisen zijn voor de data.

5.2. De eisen ten aanzien van het maximale verlies van de data ten behoeve van het veiligstellen van de data moeten zijn vastgelegd.

5.3. Bij het ontvangen van data op het platform zal er een kwaliteitstoets plaatsvinden en gedurende de periode dat de data zich op het platform bevindt zal de kwaliteit bewaakt worden voor de levensfases van de data.

5.4. De houdbaarheid van de data (retentie) moet zijn vastgelegd.

Informatiebeveiliging

Informatiebeveiliging wordt beheerst op basis van de overheidseisen. Dat is op basis van de door de overheid opgenomen Baseline Informatiebeveiliging Overheidsdiensten (BIO). Het niveau van informatiebeveiliging wordt in principe bepaald door de data die op het platform komt en vastgesteld op basis van een risicoassessment.

Atos is verantwoordelijk voor de basis security inrichting van het platform voor de publieke informatie op (Basis Informatiebeveiliging Overheidsdiensten – Basis Beveiligingsniveau 1 (BIO-BBN1) en de zwaarder beveiligde informatie op BIO-BBN2. Ter ondersteuning zal een informatiebeveiligingsrol worden gedefinieerd met twee hoofdtaken: 1) ondersteunen van het management in de inrichting van de informatiebeveiliging; 2) inhoudelijk aanspreekpunt voor informatiebeveiliging naar de diverse stakeholders.

Atos zal de informatiebeveiliging transparant maken waar dat mogelijk en gewenst is door de gemeente door het opleveren van maandelijkse informatiebeveiligingsrapportages. Voor het platform zal jaarlijks een beperkte mate van zekerheid worden gegeven ten aanzien van de opzet, bestaan en werking van de relevante securitymaatregelen uit de BIO voor de voorgenoemde Basis Beveiligingsniveaus van het standaard platform. Dit is in de vorm van een generieke ISAE3402 verklaring voor de onderliggende infrastructuurlaag en in de vorm van een specifieke auditverklaring voor standaard securityinrichting bovenop de infrastructuurlaag. Deze specifieke verklaring zal volgens gangbare auditstandaarden worden uitgevoerd en door een gecertificeerde IT auditor (RE of CISA) worden ondertekend.

Uitgangspunten

De volgende opsomming verduidelijkt op verschillende punten de bovenstaande tekst.

1. Op het platform kennen wij 2 soorten data, t.w.:
    a. Publieke data
        i. Dit is de standaard vorm van data aangezien het doel van het platform is de data te delen.
        ii. Het beveiligingsniveau is op basis van de BIO BasisBeveiligingsNiveau 1
    b. Afgeschermde data
        i. Dit is een uitzonderingssituatie. Data kunnen worden afgeschermd om 2 redenen, t.w. omdat er een commercieel belang speelt bij de eigenaar van de data of omdat de data persoonsgebonden is en dus valt binnen de AVG wetgeving.
        ii. Het beveiligingsniveau is op basis van BIO BBN2 wat voldoende is voor de persoonsgebonden data.
2. Alle data op het platform worden geregistreerd in een data-register. Hierin wordt tenminste bijgehouden:
    a. Wie de verantwoordelijke (eigenaar) is voor de data
    b. Wie de Functionaris Gegevensbescherming (FG) is voor de data (inclusief contactgegevens)
    c. Wie de verwerker is van de data
    d. Wat de doelbindingen zijn voor de data (Use Case referentie)
    e. Referentie naar het Sensorregister
    f. Referentie naar het Verwerkingsregister
    g. Referentie naar de NOK voor de Use Case
    h. Gebruikte data-elementen
3. Het platform heeft een portaalfunctie waarin voor iedere gegevensverzameling die op het platform is opgenomen is aangemerkt wie de eigenaar is en wie de FG is (bij persoonsgebonden data).
4. Op het platform is een beheerinterface aanwezig die databeheer mogelijk maakt die zowel intern als extern benaderd kan worden. Het IAM proces in beheer houdt rekening

met interne en externe beheerders die kunnen verschillen per aangeboden dataset.
In de beheerinterface voor BBN2 dienen de standaard functies voor AVG beschikbaar te zijn, d.w.z. een interface om een rapport te kunnen genereren van de persoonsgebonden informatie van een persoon, een interface om die gegevens te wijzigen en te verwijderen. (per Use Case kan de wijziging of verwijdering anders ingericht zijn. B.v. door de sensor uit het sensorregister te halen, door een nieuwe upload van de brondata te doen, et cetera)

5. De gegevensverwerker en gegevensverantwoordelijke
    a. dienen de gegevens en de applicaties op te nemen in het verwerkingsregister van het dataplatform
    b. zijn melding plichtig conform de vastgestelde procedure, indien nodig met afstemming van de betreffende Data Privacy Officer.