Responsible Sensing Lab

Verantwoord datagebruik Digitale Gracht

Thijs Turèl, Girish Vaidaya en Fabian Geiser

7 mei 2024

Management Samenvatting

De Digitale Gracht is een paar jaar geleden bedacht. Nu we een nieuwe aanbesteding cyclus naderen, is dit een gunstig moment voor een grondige herijking. Dit rapport geeft de bevindingen weer van een onderzoek dat is uitgevoerd door Responsible Sensing Lab in samenwerking met experts van Technische Universiteit Delft (TU Delft). De focus van het onderzoek lag op het evalueren en voorstellen van alternatieven voor het Digitale Gracht systeem en het bijbehorende binnenhavengeld betalingsproces, zoals gevraagd door van programma Varen. Het onderzoek is gebaseerd op niet-wettelijke normen, met name verantwoord en proportionaliteit. De term ‘verantwoord’ verwijst naar de overweging van publieke waarden zoals uiteengezet in de Amsterdamse beleidsnota's. Daarnaast omvat ‘proportionaliteit’ het beoordelen van de afstemming tussen systeemdoelen en de gebruikte methoden. Tabel 1 bevat de belangrijkste knelpunten en bijbehorende aanbevelingen die in dit onderzoek naar voren zijn gekomen.

Algemene knelpunten en aanbevelingen voor verbetering	
5.1 Afhankelijkheid van leveranciers	5.1.a Behoud systeemkennis intern
	5.1.b Verminder afhankelijkheid van één leverancier
5.2 Function creep	5.2.a Stel data stewards aan
5.3 Beperkt gedeeld begrip tussen gemeente en leveranciers	5.3.a Vereenvoudig het systeem
	5.3.b Onderhoud ‘levende documentatie’
	5.3.c Monitor de prestaties van het systeem
5.4 Beperkte bekendheid over de Digitale Gracht bij vaarweggebruikers	5.4.a Opzetten van proactieve publiekscommunicatie
5.5 Onduidelijk beleid voor toegang tot gegevens	5.5.a Beperk toegang tot data tot een ‘need-to-know’ basis
	5.5.b Beperk de afhankelijkheid van de vignetadministratie
5.6 Informatiegestuurde handhaving	5.6.a Maak niet alleen gebruik van data-gedreven prioritering van inzet van handhavers
Knelpunten en aanbevelingen voor specifieke doelstellingen	
5.7 Overmatige gegevensverzameling voor verkeersmonitoring	5.7.a Streef naar dataminimalisatie tijdens verkeersmonitoring
5.8 Proportionaliteit aanpak opsporen illegale passagiersvaart	5.8.a Heroverweeg aanpak opsporen illegale passagiersvaart
5.9 Proportionaliteit aanpak geluidsmonitoring	5.9.a Heroverweeg aanpak van geluidsmonitoring middels sensoren om geluidsoverlast te bestrijden

Tabel 1: Overzicht van de geconstateerde knelpunten en bijbehorende aanbevelingen.

Inhoud

1. Inleiding

De Digitale Gracht is een verkeersmonitoringssysteem voor de Amsterdamse binnenwateren. Het systeem dient ter ondersteuning van beleidsontwikkeling, beheer van de waterwegen en het monitoren en handhaven op het water. De Digitale Gracht, oorspronkelijk ontwikkeld in opdracht van Waternet en sinds 2020 eigendom van Gemeente Amsterdam, is recentelijk onderwerp van onderzoek geworden binnen de gemeentelijke bedrijfsvoering in discussies over publieke waarden. Hoewel sommige functies van het systeem waardevol zijn gebleken voor het monitoren van de vaarwegen, heeft het ontwerp zorgen veroorzaakt binnen de gemeente en heeft programma Varen actie ondernomen door verschillende functionaliteiten van de Digitale Gracht te deactiveren. Een uitgebreide evaluatie is nodig om de groeiende vragen over de overeenstemming van de Digitale Gracht met de doelstellingen van de gemeente op het gebied digitalisering aan te pakken.

Dit rapport presenteert de uitkomst van een onderzoek dat tot doel had alternatieven voor het Digitale Gracht systeem en het gerelateerde binnenhavengeld (ook bekend als BHG) betalingsproces te evalueren en voor te stellen. Het onderzoek is uitgevoerd door Responsible Sensing Lab in samenwerking met experts van TU Delft op verzoek van het programma Varen en richtte zich op het identificeren van knelpunten en het voorstellen van alternatieven op basis van bovenwettelijke normen met een specifieke nadruk op verantwoord en proportionaliteit. De term ‘verantwoord’ omvat de mate waarin relevante publieke waarden, zoals beschreven in Amsterdamse beleidsnota's, waaronder de Agenda Digitale Stad, de Datastrategie en het coalitieakkoord, nauwgezet zijn overwogen in de werking van dit sociaal-technische systeem. ‘Proportionaliteit’ daarentegen draait om het onderzoeken van de relatie tussen de doelen van het systeem en de methoden die worden gebruikt om deze doelen te bereiken.

Dit onderzoek beperkt zich tot de huidige staat van het Digitale Gracht systeem (september tot december 2023) en concrete voorstellen voor wijzigingen aan systemen die in ontwikkeling zijn of in het verleden zijn getest. Daarnaast strekt de scope zich uit tot het onderzoeken van de relatie tot het BHG betalingsproces. Het BHG betalingsproces werd in dit onderzoek opgenomen, hoewel het formeel niet in het Digitale Gracht systeem is geïntegreerd, maar het gedeeltelijk afhankelijk is van dezelfde technologische basis en wordt beschreven in een gezamenlijke privacyverklaring.

Dit rapport is als volgt gestructureerd. Hoofdstuk 2 introduceert de aanpak die in het onderzoek is toegepast. Hoofdstuk 3 geeft een overzicht van het Digitale Gracht systeem. Hoofdstuk 4 introduceert het BHG betalingsproces. Hoofdstuk 5 licht de geïdentificeerde knelpunten en de bijbehorende aanbevelingen voor alternatieve oplossingen toe. In hoofdstuk 6 sluit het rapport af met het presenteren van mogelijke vervolgprojecten om enkele van de meest veelbelovende alternatieven die in het vorige hoofdstuk zijn aanbevolen verder te ontwikkelen.

2. Proces

Dit hoofdstuk beschrijft de benaderingen die zijn toegepast gedurende het onderzoek in drie hoofdstappen.

2.1 Stap 1: Opbouwen van een grondig begrip van het Digitale Gracht systeem en het BHG betalingsproces

Het primaire doel van deze eerste stap was het tot stand brengen van een grondig inzicht in het Digitale Gracht systeem en de operationele complexiteiten ervan. Daarnaast richtte de focus zich op het verkrijgen van inzichten in het betalingsproces van BHG. Dit hield in dat de doelstellingen van het systeem, de belangrijkste stakeholders en operationele processen, zowel theoretisch als in de praktische uitvoering, werden verkend.

De verkenning van het Digitale Gracht systeem en de systemen die worden ingezet voor het BHG betalingsproces werd gedaan op basis van een lijst met vragen samengesteld uit 'impact assessment toolkits' IAMA (Impact Assessment Mensenrechten en Algoritmes), AIIA (AI Impact Assessment), DPIA (Data protection impact assessment) en Plot4ai. Deze hulpmiddelen zijn gekozen omdat ze worden gebruikt door de Nederlandse overheid en/of het bedrijfsleven. De vragen uit deze toolkits werden op gepaste wijze aangepast om de focus op kunstmatige intelligentie achterwege te laten. Bovendien werden alleen beschrijvende vragen (d.w.z. vragen die onderzoeken *hoe* een systeem werkt en *waarom*) overwogen. De volledige vragenlijst is te vinden in Bijlage 1. Informatie over het Digitale Gracht systeem en BHG proces werd verzameld uit zeven semi gestructureerde interviews met in totaal tien deelnemers die een cruciale rol spelen in de ontwikkeling en het gebruik van het Digitale Gracht systeem.

De lijst van deelnemers omvat vertegenwoordigers van:

- Nautisch Beleid (programma Varen);
- Nautisch Beheer (programma Varen);
- Nautisch Toezicht en Handhaving in de Openbare Ruimte (THOR);
- ICT-team van het programma Varen;
- Global Guide Systems (leverancier);
- PortPay (leverancier).

Verder werden relevante documentatie, zoals de privacyverklaring en DPIA, met betrekking tot het Digitale Gracht systeem bestudeerd. De informatie die werd verzameld uit de interviews en documenten werd verfijnd door vervolg vergaderingen en e-mails met de geïnterviewden.

Ten slotte werd een beschrijving van de Digitale Gracht en BHG betaalsysteem opgesteld op basis van de verzamelde informatie en geverifieerd met alle deelnemers aan de interviews.

2.2 Stap 2: Identificeren van knelpunten en verbetermogelijkheden

De verkenning van knelpunten en verbetermogelijkheden in verband met het Digitale Gracht systeem en BHG betalingsproces was een gezamenlijke inspanning van het team van Responsible Sensing Lab, in samenwerking met Marijn Janssen (Professor in ICT & Governance) en Kars Alfrink (onderzoeker Contestable AI) van TU Delft. Voortbouwend op een grondig begrip van deze

systemen, putte de gezamenlijke analyse uit de expertise van alle samenwerkende partijen, waarbij inzichten uit eerdere projecten en beleidsrichtlijnen die door Gemeente Amsterdam worden omarmd, zoals de Agenda Digitale Stad, meegenomen. Bovendien werden gevestigde kaders uit relevante literatuur, waaronder de “Data Governance Principles” (Janssen et al., 2020) en “Contestable AI by Design” (Alfrink et al., 2022) raamwerken toegepast om systematisch potentiële knelpunten en verbetermogelijkheden te identificeren. Een aantal knelpunten en verbetermogelijkheden werd bovendien benadrukt door de betrokken medewerkers van het programma Varen van Gemeente Amsterdam.

2.3 Stap 3: Aanbevelen van alternatieven

De aanbevelingen voor alternatieven voor de Digitale Gracht en het BHG betaalsysteem zijn geformuleerd als reactie op de problemen die zijn geïdentificeerd in stap 2. Dit werd gedaan in samenwerking met Prof. Marijn Janssen, Kars Alfrink en Sander Flight (Privacy expert van Responsible Sensing Lab).

3. Het Digitale Gracht systeem

Dit hoofdstuk geeft een overzicht van het Digitale Gracht systeem. De informatie die in dit hoofdstuk wordt gepresenteerd dient, samen met de beschrijving van het BHG betalingsproces in hoofdstuk 4, als basis voor de knelpunten en verbetermogelijkheden die in dit onderzoek zijn geïdentificeerd.

3.1 Doelstellingen en gerelateerde systemen

Het Digitale Gracht systeem heeft vijf hoofddoelstellingen, die hieronder worden gepresenteerd in volgorde van belangrijkheid zoals aangegeven door het Digitale Gracht-team:

1. Inzicht in de drukte op de grachten;
2. Terugdringen van illegale passagiersvaart;
3. Verminderen van geluidsoverlast op het water;
4. Terugdringen van snelheidsovertredingen;
5. Reguleren van aanlegplaatsen voor commerciële vaartuigen.

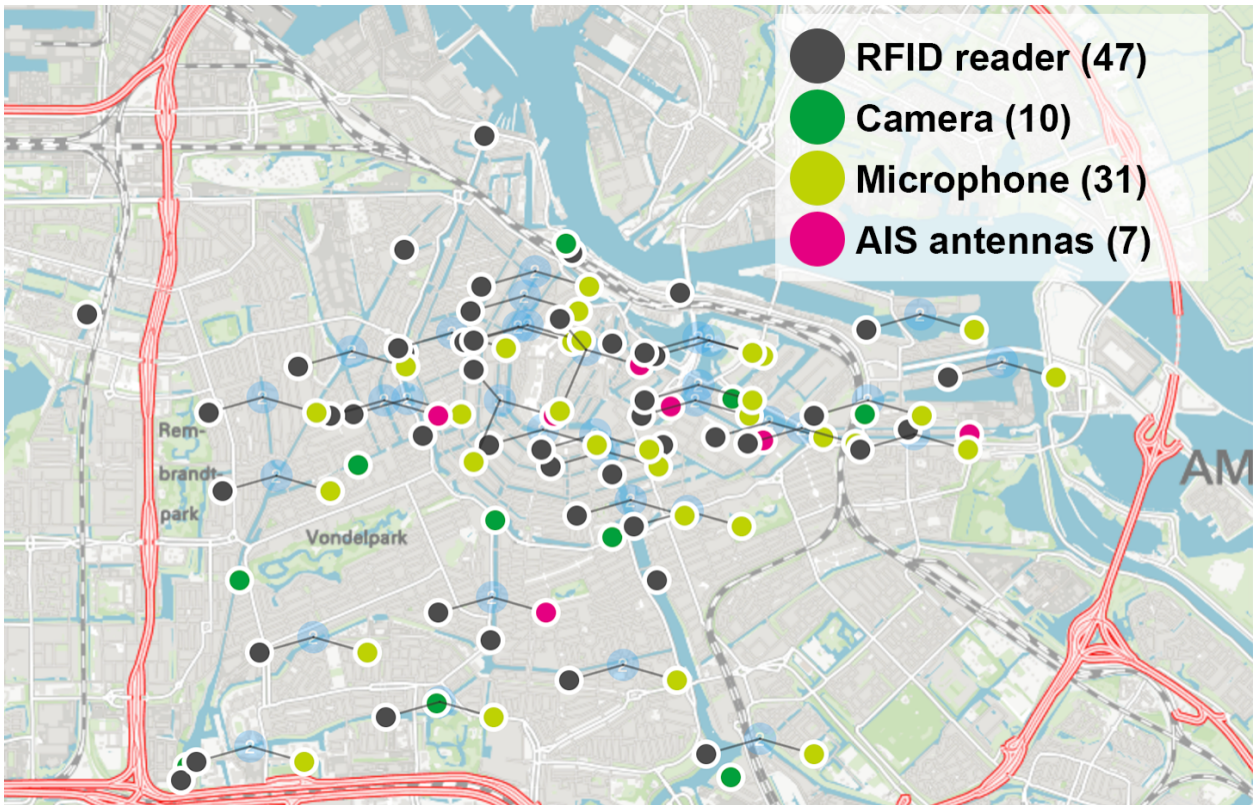
1. Inzicht in de drukte in de grachten

Ter ondersteuning van de wettelijke taak om vlot en veilig verkeer op het water te waarborgen heeft Gemeente Amsterdam een uitgebreid systeem geïmplementeerd voor het monitoren van het waterverkeer. Het systeem betreft commerciële, private en niet-gemotoriseerde vaartuigen en draagt bij aan het voorkomen van overlast, het vergroten van de leefbaarheid en het optimaal benutten van de vaarwegen van de stad.

De Digitale Gracht maakt gebruik van verschillende sensoren om informatie te verzamelen over activiteiten op het water:

- **RFID-lezers en vignetten**: Deze apparaten registreren passages door chips in vignetten te detecteren (vignetten zijn verplicht voor gemotoriseerde vaartuigen). Bij elke passage worden het unieke hardwarenummer, het tijdstip, de sensor-ID en de richting van het vaartuig vastgelegd.
- De door de RFID-lezers verzamelde gegevens worden geclassificeerd naar type vignet (bijvoorbeeld pleziervaart of passagiersvaart) met behulp van het hardwarenummer door het te koppelen aan de BHG database. Deze database is een lijst van hardwarenummers en de bijbehorende vaartuigcategorieën. (Dit is een database die los staat van de vignetadministratie. Meer hierover in hoofdstuk 4).
- **Camera's** worden gebruikt om vaartuigen zonder vignet te identificeren waarbij passages, tijdstip, sensor-ID's en richtingen worden geregistreerd.
- **AIS transponders en antennes** worden gebruikt om het verkeer van commerciële en grotere privévaartuigen te monitoren en de drukte per traject te bepalen. AIS-gegevens zijn in Nederland verplicht voor commerciële vaartuigen en voor particuliere vaartuigen met een lengte van minstens 20 meter, waarvan de gegevens bijna realtime zichtbaar zijn. AIS antennes registreren informatie, waaronder het MMSI-nummer (Maritime Mobile Service Identity Number), dat fungeert als vaartuig-ID, evenals de locatie, tijdstip, richting en snelheid van het vaartuig. Deze gegevens worden elke vijf tot vijftien seconden vastgelegd. Aanvullende details zoals de naam van het vaartuig, het type, de grootte en de vlag worden met lagere frequentie verzameld. AIS-gegevens worden beschouwd als persoonsgegevens omdat er mensen kunnen wonen op de boten die gemeten worden.

Een overzicht van de verdeling van de sensoren die voor de Digitale Gracht worden gebruikt, is te zien in Figuur 1. Figuur 2 toont een voorbeeld van een Digitale Gracht sensor.



Figuur 1 - Overzicht van de plaatsing, het type en de hoeveelheid (tussen haakjes) van sensoren die worden gebruikt voor het Digitale Gracht systeem, afkomstig van sensorenregister.amsterdam.nl. Kanttekening: dit overzicht geeft de situatie in 2022 weer. Sindsdien zijn er enkele wijzigingen doorgevoerd.

2. Terugdringen van illegale passagiersvaart

Het specifieke doel van dit onderdeel van het systeem is het identificeren van privévaartuigen die betrokken zijn bij illegale passagiersvaart, voor commercieel vervoer van passagiers is een vergunning vereist. Om dit te bereiken is er een ‘rule-based’ algoritme ontwikkeld dat door middel van profilering vaartuigen detecteert die verdacht worden van het aanbieden van passagiersvaart de vereiste vergunning. Dit algoritme is momenteel niet actief (zie figuur 3 en tabel 2). De intentie was om de door RFID-lezers verzamelde gegevens te verwerken om vaartuigen te identificeren die repetitieve vaarpatronen vertonen. Verdachte vaartuigen die met dit algoritme werden geïdentificeerd, werden opgenomen in een wekelijks verslag.

3. Verminderen van geluidsoverlast op het water

Het probleem van geluidsoverlast op en rondom het water van Amsterdam is duidelijk aanwezig, zoals blijkt uit meldingen van bewoners die zijn opgeslagen in het gemeentelijke incidentmeldingssysteem ‘Signalen in Amsterdam’ (SIG). Als reactie hierop streeft de gemeente ernaar geluidsoverlast veroorzaakt door vaarweggebruikers aan te pakken via het Digitale Gracht systeem.

Tot voor kort werden geluidsgebeurtenissen op de grachten geregistreerd met behulp van AllSense-sensoren. Deze sensoren zijn een combinatie van een RFID-lezer, een camera en twee microfoons. De camera en microfoons in de AllSense-sensoren zijn op het moment van schrijven inactief. AllSense registreerde het tijdstip, de sensor-ID (en daarmee de locatie) en het dB-niveau van

geluidsgebeurtenissen, wat aangaf wanneer een specifieke dB-drempel werd overschreden op een specifieke tijd en plaats.

Om geluidsovertredingen door een individueel vaartuig te detecteren, werd enkele jaren geleden een geluidsmonitoring rapportage ontwikkeld en getest. Deze toepassing is momenteel ook niet actief. De rapportage baseerde zich op gegevens van de AllSense-sensoren. In het geval van een geluidsgebeurtenis op het water werden audio, video, sensor-ID, tijd en unieke hardwarenummer van het vaartuig dat tijdens de geluidsgebeurtenis aanwezig was, vastgelegd.

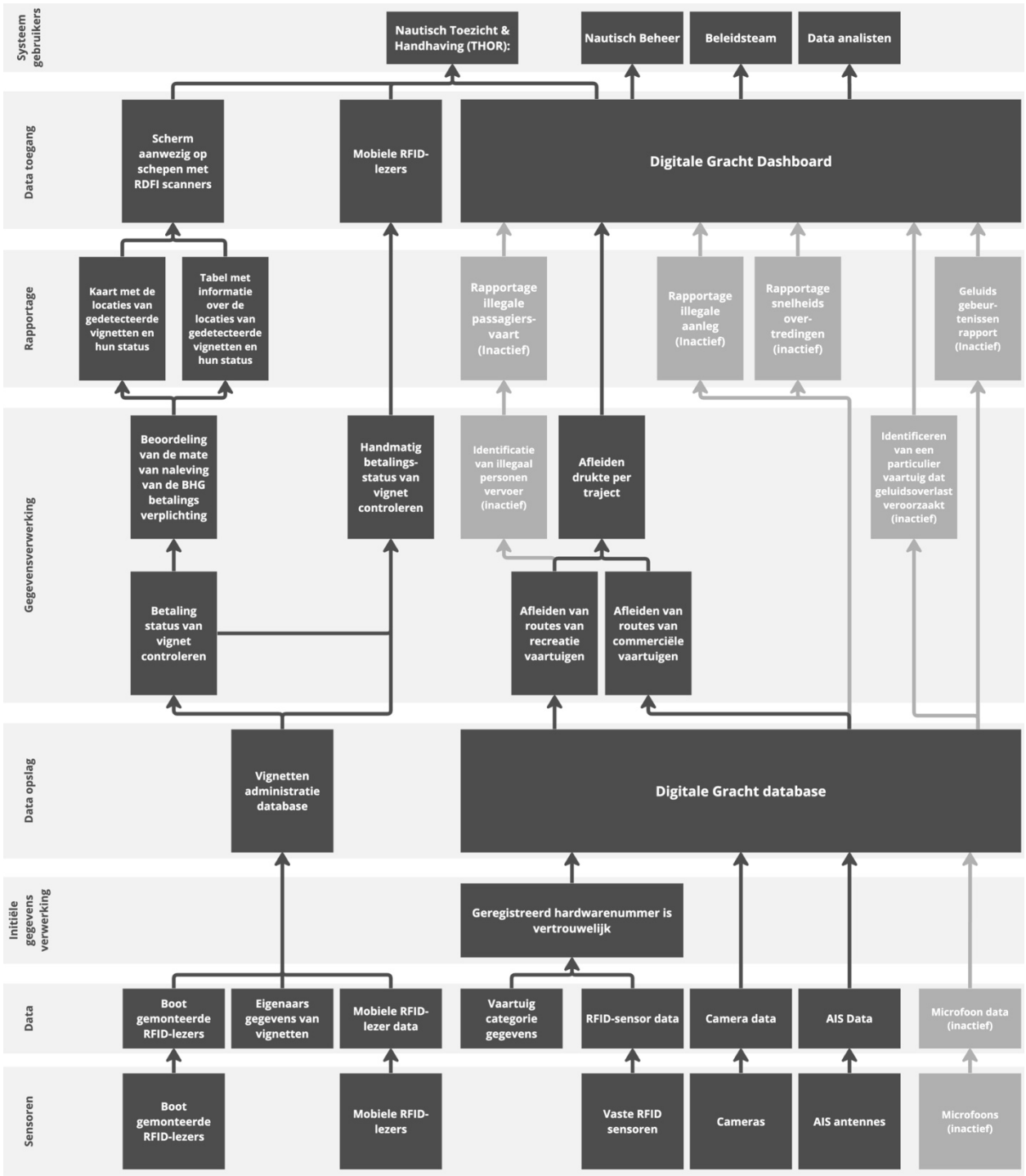
Figuur 2 - Een Digitale Gracht sensor en referentiesticker (in het rode vierkant) op het Marineterrein Amsterdam. De sensor op de foto is een AllSense-sensor.

4. Terugdringen van snelheidsovertredingen

Gemeente Amsterdam wil het aantal snelheidsovertredingen door commerciële vaartuigen in de vaarwegen verminderen. Het Digitale Gracht systeem was oorspronkelijk ontworpen om dergelijke overtredingen te detecteren met behulp van AIS-gegevens. De AIS-gegevens die door de Digitale Gracht worden verzameld, bieden inzicht in de snelheid, de locatie en het unieke MMSI-nummer van commerciële vaartuigen. Het was bedoeld dat een algoritme deze gegevens zou benutten om snelheidsovertredingen te monitoren en rapportages te genereren om vaartuigen te identificeren die betrokken waren bij dergelijke overtredingen. De informatie over de snelheid van vaartuigen blijft toegankelijk via het dashboard, maar de functie voor het automatisch genereren van rapporten is momenteel gedeactiveerd.

5. Reguleren van aanlegplaatsen voor commerciële vaartuigen

Commerciële vaartuigen (zoals passagiersvaartuigen en transportvaartuigen) mogen alleen afmeren op de aan hen vergunde ligplaatsen of in jachthavens. Het Digitale Gracht systeem was bedoeld om vaartuigen die ‘s nachts buiten deze plekken afmeren te identificeren en te rapporteren. Als een vaartuig zich tijdens deze uren buiten de toegestane ligplaats of veilige zone bevindt, wordt dit in het dagelijkse rapport opgenomen. Het is belangrijk op te merken dat deze functionaliteit momenteel gedeactiveerd is.



Figuur 3 - Overzicht van de gegevensverzameling en gegevensverwerking uitgevoerd in het kader van de Digitale Gracht.

Functionaliteit	Status
1. Actueel druktebeeld	Beschikbaar
2. Detectie geluidsoverlast	Gedeactiveerd
3. Detectie illegale passagiersvaart	Gedeactiveerd
4. Indicator snelheidsovertreding	Beschikbaar voor beroepsvaart
5. Detectie illegaal gebruik ligplaatsen	Gedeactiveerd

Tabel 2: Overzicht van de Digitale Gracht functionaliteiten en hun status.

3.2 Interne stakeholders

De stakeholders die binnen de gemeente actief betrokken zijn bij het toezicht op en de werking van het Digitale Gracht systeem zijn ‘programma Varen’ en ‘Toezicht en Handhaving in de Openbare Ruimte’ (THOR). Deze organisatieonderdelen vervullen verschillende rollen bij het beheer en gebruik van de gegevens die door het Digitale Gracht systeem worden verzameld.

1. Programma Varen

Programma Varen, de gemeentelijke partij die verantwoordelijk is voor de Digitale Gracht, is de ‘eigenaar’ van de verzamelde gegevens. Dit programma bestaat uit verschillende teams die betrokken zijn bij het Digitale Gracht systeem:

- ICT-team: Verantwoordelijk voor het formuleren van de eisen van de Digitale Gracht, het coördineren van wijzigingen met leveranciers en het beheren van accounts voor het Digitale Gracht dashboard.
- Beleidsteam: Gebruikt inzichten uit de Digitale Gracht om bestaand beleid te evalueren, onderbouwen, herzien en mogelijk nieuwe beleidsmaatregelen voor te stellen met betrekking tot verkeer, vergunningen voor commerciële vaartuigen, geluid, snelheid en ligplaatsen. Dit team zorgt ervoor dat bewoners, ondernemers en bezoekers niet onevenredig worden getroffen door beleidswijzigingen.
- Nautisch Beheer: Geïnteresseerd in de verzamelde informatie om korte termijn interventies te informeren en te rechtvaardigen, zoals stremmingen van vaarwegen of ontheffingen tijdens werkzaamheden of evenementen zoals het Prinsengrachtconcert .

2. Nautisch Toezicht en Handhaving

Het team Nautisch Toezicht en Handhaving van Toezicht en Handhaving in de Openbare Ruimte is verantwoordelijk voor het handhaven van de regelgeving en gebruikt Digitale Gracht gegevens voor monitoring en interventie:

- Monitort snelheids-, aanmeer- en geluidsovertredingen en spoort illegale passagiersvaart op.
- Verantwoordelijk voor het opleggen van boetes aan overtreders en geïnteresseerd in informatiegestuurde inzet van BOA's (Buitengewoon Opsporings Ambtenaar) en het versturen van waarschuwingen naar vaartuigen die overtredingen begaan.

3. Leveranciers

Het Digitale Gracht systeem wordt ontwikkeld en onderhouden door twee leveranciers: Global Guide Systems (GGS) en PortPay, een handelsnaam van Improvement IT.

- GGS is een kleinschalige organisatie die verantwoordelijk is voor de ontwikkeling en het beheer van de functionaliteiten van het Digitale Gracht systeem, waaronder het dashboard. GGS is eigenaar van de softwarecode van de Digitale Gracht applicaties en verzamelt AIS data.
- PortPay is een subleverancier die sensoren (met uitzondering van AIS ontvangers en antennes) levert voor het Digitale Gracht systeem. PortPay is verantwoordelijk voor het systeemonderhoud en voert de initiële gegevensverwerking en filtering uit voordat de gegevens naar GGS worden doorgestuurd.

3.3 Het Digitale Gracht dashboard

De informatie die voortkomt uit de gegevens verzameld door het Digitale Gracht systeem wordt beschikbaar gesteld in het Digitale Gracht dashboard. Toegang tot dit dashboard wordt uitsluitend verleend via persoonlijke accounts die worden beheerd door het ICT-team, waarbij de toegankelijkheid beperkt is tot medewerkers van de gemeente. Momenteel hebben bepaalde BOA's van Nautisch Toezicht en Handhaving, beleidsadviseurs, nautisch beheer en onderzoekers (zoals data-analisten van de gemeentelijke afdeling Verkeer en Openbare Ruimte) accounts. Via deze accounts is alle onderstaande informatie toegankelijk. Onderzoekers kunnen bovendien ruwe gegevens downloaden. Volgens GGS heeft de gemeente de mogelijkheid om de toegang binnen het dashboard te verfijnen. Deze functionaliteit wordt momenteel niet gebruikt.

Gemeente Amsterdam wisselt geen persoonsgegevens uit die in het kader van de Digitale Gracht verzameld zijn met andere organisaties. In het verleden hebben andere organisaties, zoals de politie, interesse getoond in het verkrijgen van toegang tot (delen van) de gegevens. Op het dashboard is de volgende informatie toegankelijk.

- Gegevens verzameld door sensoren:
    - De status van het vignet (of het verlopen is of niet).
    - Het type vignet (bijvoorbeeld passagiersschip).
    - Het unieke hardwarenummer van vaartuigen met vignetten waarvoor in de afgelopen 72 uur een passage is geregistreerd door een RFID-lezer. Routes die door privévaartuigen zijn afgelegd (gebaseerd op RFID-gegevens) zijn niet direct zichtbaar op het dashboard, maar kunnen worden afgeleid uit de hardwarenummers die in een lijst zijn opgenomen.
    - MMSI-nummer, naam van het vaartuig, grootte van het vaartuig, huidige locatie, afgelegde route in de afgelopen 72 uur, snelheid en naam van het vaartuig van commerciële en grote particuliere vaartuigen.
    - Geluidsgebeurtenissen op specifieke locaties (kleurindicator).
- Rapportages (momenteel zijn er geen rapportages toegankelijk):
    - Rapporten over illegaal passagiersvervoer.
    - Geluidsrapporten.
    - Snelheidsrapporten.
    - Rapporten over illegaal aanmeren.

3.4 Relatie met burgers

Burgers worden geïnformeerd over het Digitale Gracht systeem door middel van officiële stickers die naast de sensoren in de openbare ruimte zijn geplaatst, en door middel van gegevens over de sensoren in het sensorenregister en een online privacyverklaring. Het sensorenregister en de privacyverklaring blijken enigszins verouderd te zijn. Onlangs is een beschrijving van de gebruikte algoritmen toegevoegd aan het algoritmen register van Gemeente Amsterdam. Bij aankoop van een vignet ontvangen vaartuigeigenaren een brief die verwijst naar een video op de website van de gemeente. In de video wordt vermeld dat de vignetten chips bevatten die de gemeente helpen bij het monitoren van het verkeer.

Burgers kunnen vragen stellen over de sensoren en klachten indienen via de contactgegevens die op de stickers en in het sensor register worden verstrekt. Er zijn geen formele processen voor bezwaar, rectificatie, inspectie of verwijdering. In zijn huidige vorm biedt het systeem burgers geen kanalen om toegang te krijgen tot informatie over hun vaartuigen, behalve de openbaar beschikbare AIS-gegevens die voor grotere vaartuigen worden verzameld.

4. Het Binnenhavengeld (BHG) betalingsproces

In dit hoofdstuk wordt het BHG betalingsproces toegelicht. De beschrijving in dit hoofdstuk dient, samen met de verzamelde kennis over het Digitale Gracht systeem in het vorige hoofdstuk, als basis voor de knelpunten en verbetermogelijkheden die in dit rapport worden geïdentificeerd.

Gemeente Amsterdam heeft een systeem geïmplementeerd om naleving van de BHG betalingsverplichting voor eigenaren van pleziervaartuigen die gebruik maken van het water en aanmeren in de stad te handhaven. De belangrijkste doelstellingen zijn het controleren of voor pleziervaartuigen BHG is betaald en het versturen van aanmaningen. Daarvoor is het nodig om ook een indicatie te hebben van de mate waarin mensen de BHG verplichting naleven.

PortPay heeft van de gemeente de opdracht gekregen om het BHG registratie- en incassoproces te beheren. Voor elk aangeschaft vignet verzamelt PortPay de volgende gegevens: naam, adres en woonplaats (NAW); burgerservicenummer (BSN) en betalingsgegevens van de persoon die de aankoop doet; hardwarenummer van de RFID-chip en licentienummer van het vignet; foto's van het vaartuig waarvoor BHG is betaald. De verzamelde gegevens worden opgeslagen in de vignetadministratie database die door PortPay wordt beheerd.

BHG controles worden uitgevoerd door BOA's van Nautisch Toezicht en Handhaving. Voor handhaving worden BOA's ingezet op basis van een rasterbenadering voor steekproeven (evenwijdige verdeling van controles over de stad) om vaartuigen in deze gebieden handmatig te inspecteren. Handscanners geven BOA's toegang tot de vignetadministratie, waarbij persoonlijke informatie over de eigenaar wordt verstrekt. In het geval van een overtreding van de betaalvignetverplichting wordt een vaartuigeigenaar via sms op de hoogte gesteld mits op het vaartuig een vignet is bevestigd. Is er geen vignet, dan is de eigenaar niet bekend. Wanneer binnen de gestelde termijn niet wordt betaald, kan het vaartuig worden weggesleept.

Dienstvaartuigen van Nautisch Toezicht en Handhaving zijn uitgerust met vignet-lezers die het aantal vignetten tellen dat aan vaartuigen is bevestigd. Eens per jaar vergelijken ze het aantal vignetten dat door de sensor is geteld met het aantal vaartuigen dat door BOA's in het veld is geteld om inzicht te krijgen in de naleving van de BHG plicht en het totale aantal vaartuigen met en zonder vignet dat op het water aanwezig is. Om de mate van naleving van de BHG betalingsverplichting te bepalen, worden bovendien passagetellingen van camera's vergeleken met RFID-sensor tellingen om vaartuigen zonder geldige vignetten te identificeren. Camera's registreren alleen passages, wat betekent dat er geen onderscheid kan worden gemaakt tussen vaartuigen die geen BHG vignet nodig hebben, zoals kajaks, en vaartuigen die de BHG betalingsverplichting schenden en geen BHG vignet hebben aangeschaft.

5. Knelpunten en aanbevelingen voor alternatieven

Dit hoofdstuk schetst de knelpunten die zijn geïdentificeerd door Responsible Sensing Lab in samenwerking met prof. Marijn Janssen en onderzoeker Kars Alfrink (TU Delft). Voor elk probleem geven we één of meer aanbevelingen voor alternatieve benaderingen. Het hoofdstuk bestaat uit twee delen: het eerste deel behandelt algemene kwesties en aanbevelingen voor de Digitale Gracht en het BHG betalingsproces, terwijl het tweede deel in gaat op kwesties en aanbevelingen voor de specifieke doelstellingen die in hoofdstuk drie en vier van dit rapport zijn geïntroduceerd.

Algemene knelpunten en aanbevelingen voor alternatieven

5.1 Afhankelijkheid van leveranciers

Het is gebruikelijk dat steden gebruikmaken van de diensten van technologische dienstverleners en leveranciers. Dit brengt noodzakelijkerwijs een afhankelijkheid met zich mee. Toch moet een ‘lock-in’ worden vermeden en de machtsbalans worden aangepakt. De verdeling van werkzaamheden in de huidige aanbesteding heeft geleid tot een situatie waarin de ene leverancier en zijn toeleverancier een aanzienlijke mate van controle hebben over het systeem in vergelijking met Gemeente Amsterdam. De kennis van het technische systeem ligt voornamelijk bij de leveranciers en niet bij het personeel van de gemeente. Dit brengt verschillende risico's met zich mee.

De gemeente is verantwoordelijk voor de dagelijkse werking van het systeem, maar beschikt niet over de beste informatiepositie om de werking te begrijpen en de risico's af te wegen die hiermee gepaard gaan. Dit is vooral belangrijk in onvoorziene situaties. Mochten de huidige leveranciers niet langer beschikbaar zijn (bijvoorbeeld bij een faillissement), dan kan het ontbreken van gedocumenteerde kennis problematisch zijn. Het voorkomt dat de stad (een deel van) het werk overneemt (Hubert, 2020, 2022).

Zelfs bij een geplande verschuiving van leveranciers (bijvoorbeeld bij een nieuwe aanbestedingsperiode) maakt de vastgelegde kennis van het systeem het moeilijk voor een andere leverancier om het systeem over te nemen zonder ondersteuning van GGS en PortPay. Het systeem is door de verkoper op maat gemaakt voor deze toepassing, wat betekent dat de sensoren en de software niet op de markt verkrijgbaar zijn. Het ontbreekt de stad mogelijk aan de nodige kennis om de inkomende biedingen van concurrenten te beoordelen op hun technische haalbaarheid.

Bovendien kan een te grote afhankelijkheid van een paar leveranciers innovatie beperken, de kosten verhogen en de veiligheid beïnvloeden, omdat leveranciers gebonden zijn aan de economische wetmatigheid om te leveren wat de aanbesteding vereist, maar niet meer dan dat. Tot slot, een klein maar mogelijk veiligheidsrisico wordt gevormd door de mogelijkheid dat een leverancier wordt overgenomen door een bedrijf dat gevestigd is in een niet-Europees, niet-vriendelijk land.

Geïnspireerd door:

- *Agenda Digitale Stad 2023-2026, ambitie digitale afhankelijkheid (Gemeente Amsterdam, 2023).*
- *Amsterdamse Datastrategie, Legitiem en gecontroleerd 'belangrijk dat datastromen controleerbaar zijn' (Gemeente Amsterdam, 2021)*.

5.1.a Aanbeveling: Behoud systeemkennis intern

Voor de komende aanbestedingsronde adviseren we om een deel van het ‘waardeketen'-werk dat nu aan leveranciers wordt uitbesteed, in te houden om interne kennis te behouden en innovatief te blijven.

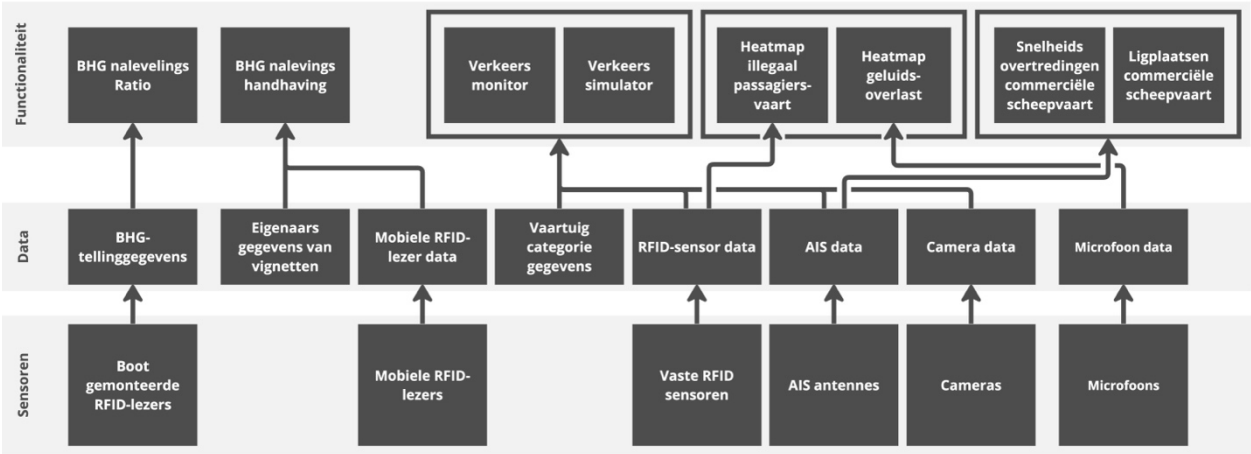
We stellen ons bijvoorbeeld voor dat er een intern ontwerp/ontwikkel/operation team wordt opgezet dat applicaties die gebruik maken van de sensordata bouwt en onderhoudt, waarbij de beschikbaarheid van werkende sensoren wordt ingekocht in de markt.

Gemeente Amsterdam experimenteert met een dergelijke opzet bij het Computer Vision Team van de Innovatieafdeling. Daar is met succes een aanbesteding uitgeschreven waarbij de meer ‘high-end’ taken intern worden belegd, terwijl het minder kritische/eenvoudiger te vervangen werk wordt uitbesteed.

5.1.b Aanbeveling: Verminder afhankelijkheid van één leverancier

Wed niet op één paard. Als de volledige technologische ondersteuning bij één leverancier is ondergebracht, kan dit problematisch worden in een situatie waarin de leverancier niet levert.

Als alternatief kan worden overwogen om de verschillende toepassingen bij verschillende leveranciers onder te brengen. Figuur 4 toont een voorgesteld diagram voor de systeemarchitectuur. Eén toepassing kan bijvoorbeeld worden gebruikt voor het monitoren van de huidige verkeerssituatie, waarbij gebruik wordt gemaakt van RFID- en AIS-gegevens. Een andere toepassing kan worden gebruikt voor analyse of simulatie van verkeersinterventies, waarbij dezelfde gegevens worden gebruikt als bij verkeersmonitoring, inclusief historische gegevens. Verdere toepassingen kunnen handhaving ondersteunen; handhaving gericht op particulieren, voor zaken als illegale passagiersvaart of geluidsoverlast, of handhaving met betrekking tot commerciële bedrijven, voor zaken als snelheidsovertredingen en aanlegplaatsen. AIS-gegevens dienen voorzichtig worden te gebruikt, omdat het systeem alleen werd geïntroduceerd voor identificatie en positiebepaling van vaartuigen, zoals in 2006 is vastgelegd in het convenant tussen het ministerie van Verkeer en Waterstaat en de binnenvaartsector (Bureau Telematica Binnenvaart, 2024).



Figuur 4 - Voorgesteld diagram voor systeemarchitectuur. Dit diagram geeft een voorgestelde departementalisatie weer inclusief functionaliteiten die in dit rapport worden aanbevolen om te heroverwegen. Kleuren geven afzonderlijke doelen aan. Verantwoordelijkheden en toegang kunnen worden verdeeld langs verticale (beleidsdoelen) of horizontale (sensoren/gegevens/functionaliteit) lijnen.

5.2 Function creep

Het komt vaak voor dat digitale systemen worden gebruikt voor doeleinden waarvoor ze oorspronkelijk niet bedoeld waren. In een democratische organisatie wordt dit ‘function creep’ genoemd. Volgens Bert-Jaap Koops, Prof. Regulering & Technologie aan de Universiteit van Tilburg, verwijst function creep naar een scenario waarin het gevoel heerst dat er onvoldoende gelegenheid is geweest voor discussie over de wenselijkheid van een nieuwe functie vóór de implementatie ervan (Koops, 2021).
Bij digitale systemen, in vergelijking met fysieke systemen, is er een toegevoegd risico op function creep omdat het aantal betrokkenen, de benodigde inspanning en kosten om substantiële veranderingen aan te brengen die een systeem meer invasief kunnen maken, zeer laag kunnen zijn. Het wijzigen van enkele regels code, het wijzigen van toegangsrechten of aggregatieniveaus, het toevoegen van een nieuwe tab aan een dashboard waarin bepaalde gegevens worden gecombineerd, kan ernstige gevolgen hebben, maar kan snel worden uitgevoerd. In een situatie waarin leveranciers hun eigen beslissingen kunnen nemen, zouden nieuwe functies onopgemerkt kunnen blijven door Gemeente Amsterdam.

De ultieme bescherming tegen function creep is een continue democratische legitimering voor veranderingen in het systeem. Naarmate de kosten voor het doorvoeren van technologische veranderingen dalen, is het de moeite waard om barrières te ontwerpen voor onbedoelde veranderingen.

Geïnspireerd door:

- *Tada principe: Democratisch en legitiem (tada.city, 2017).*

5.2.a Aanbeveling: Stel data stewards aan
Kenniscompartimentering helpt om onbedoeld gebruik van data te voorkomen. Data stewards, oftewel gegevensbeheerders, kunnen hierbij een essentiële rol spelen. Om de gemeente in staat te stellen controle over haar eigen gegevens te behouden, moeten gegevensbeheerders afkomstig zijn van Gemeente Amsterdam.

Overweeg bijvoorbeeld om het systeem op te splitsen met één data steward voor elke gegevensbron of sensortype, zoals sensor hardware, RFID, geluid, camera's en andere gegevensbronnen zoals vignetten en AIS (zie figuur 4). Een data steward is een rol die verantwoordelijk is voor de gegevens die hij verzamelt en verwerkt, om ervoor te zorgen dat deze alleen worden gebruikt voor het beoogde doel en alleen door geautoriseerde personen, die intern of bij leveranciers kunnen zijn geplaatst. Deze stewards zijn de exclusieve beheerders van hun respectievelijke datasets en ze zijn verplicht om de transparantie van datatoegang te handhaven door te loggen wie welke data wanneer gebruikt.

5.3 Beperkt gedeeld begrip tussen gemeente en leveranciers

Leden van het Digitale Gracht-team hebben niet altijd volledige kennis over de huidige functionele status en ook is er geen volledige up-to-date documentatie. Terwijl sommige geïnterviewden van de gemeente bijvoorbeeld geloofden dat radars nog steeds actief waren en gebruikt werden om passages te registreren, vertelden de leveranciers ons dat radars al enige tijd geleden waren uitgeschakeld.

Het is noodzakelijk dat het personeel van Gemeente Amsterdam een grondig begrip heeft van het technische systeem als voorwaarde om controle te houden en verantwoordelijkheid te nemen. Het gebrek aan gedeeld begrip kan worden toegeschreven aan de complexiteit van het systeem en de

vele wijzigingen die er in de loop van de levensduur zijn aangebracht. Onvoldoende actuele documentatie maakt het probleem nog groter. Naast de uitdagingen voor de gemeentelijke organisatie, maakt deze situatie het ook ingewikkelder voor individuen die niet tot de gemeentelijke organisatie behoren om de lopende ontwikkelingen te begrijpen.

Geïnspireerd door:

- *Amsterdamse Datastrategie, Legitiem en gecontroleerd 'belangrijk dat datastromen controleerbaar zijn' (Gemeente Amsterdam, 2021).*

5.3.a Aanbeveling: Vereenvoudig het systeem

Vereenvoudig het systeem zoveel mogelijk. Wij stellen dat een eenvoudiger systeem duidelijkheid biedt voor het projectteam, waarbij wordt afgebakend wat het wel en niet kan bereiken. Bovendien vergemakkelijkt vereenvoudiging externe controle, waardoor de reputatie van het project wordt beschermd en PR-risico's worden beperkt. Wij geloven dat de complexiteit van het Digitale Gracht systeem voortkomt uit ten minste twee kenmerken. Ten eerste is het systeem complex vanwege het aantal verschillende doelen en de integratie van deze verschillende doelen. Een voorbeeld hiervan is het gebruik van unieke elektronische ID's voor verkeersmonitoring en het controleren van betalingen van BHG. Het opsplitsen van het systeem zoals voorgesteld in figuur 4 zou kunnen helpen om de complexiteit te verminderen die wordt veroorzaakt door de verstrengeling van doelstellingen en technische oplossingen. Ten tweede dragen sommige van de specifieke oplossingen die zijn gekozen om bepaalde functionaliteiten mogelijk te maken bij aan de complexiteit van het Digitale Gracht systeem. Een voorbeeld hiervan is de huidige aanpak van verkeersmonitoring, die gebruik maakt van een verscheidenheid aan sensoren en verwerkingsmethoden, waaronder het registreren van passages van individuele vaartuigen en het afleiden van de route die deze vaartuigen waarschijnlijk hebben afgelegd. Wij zijn van mening dat een oplossing die gebruikmaakt van één type sensor en simpelweg passages telt, de complexiteit vermindert en voor alle stakeholders gemakkelijker te begrijpen is. Daarom adviseren we om oplossingen te kiezen die eenvoudig en gemakkelijk te begrijpen zijn, in plaats van complexe oplossingen die extra uitleg vereisen.

5.3.b Aanbeveling: Onderhoud 'levende documentatie'

We raden aan dat de documentatie over het systeem continu bijgewerkt wordt. Deze documentatie moet een integraal onderdeel zijn van zowel de ontwikkelings- als de operationele workflows. Nieuwe functies dienen volledig worden gedocumenteerd en openbaar worden gemaakt (bijvoorbeeld door de functies bekend te maken via het algoritme register) voordat ze worden geïmplementeerd, gezien vanuit het perspectief van het publiek of een publieke vertegenwoordiger. Een sensor zou bijvoorbeeld alleen kunnen worden geactiveerd als deze officieel is opgenomen in het sensor register. Het is mogelijk om een dergelijke voorwaarde af te dwingen door controles in de technische workflow te integreren. In dit specifieke geval kan het software algoritme de geldige sensoren lezen uit het sensor register en vervolgens alleen de geregistreerde gegevens verwerken. Kortom, alle gegevens die wel door een sensor worden geregistreerd maar niet zijn opgenomen in het sensor register, worden automatisch genegeerd.

We raden aan om twee soorten documentatie bij te houden: één voor intern gebruik en een andere voor het publiek, die toegankelijk moet zijn via het online algoritmeregister van Amsterdam. Het is belangrijk om ervoor te zorgen dat elke nieuwe functie die aan het systeem wordt toegevoegd uitvoerig gedocumenteerd wordt.

5.3.c Aanbeveling: Monitor de prestaties van het systeem
Voer kwaliteitscontroles uit na de implementatie van het systeem. Dit houdt in dat prestatie indicatoren worden gebruikt om de effectiviteit van het systeem te meten. Deze indicatoren moeten gekoppeld zijn aan de ontwikkelingsfase van het systeem en worden vastgesteld in overeenstemming met normen zoals wetten voor gegevensbescherming. De indicatoren moeten zowel functionele doelstellingen als op publieke waarden gebaseerde standaarden weerspiegelen. Functionele doelstellingen hebben betrekking op het doel van het systeem en sommige functionele doelstellingen worden momenteel al gemonitord, zoals de nauwkeurigheid van de vaartuigdetectie, die de basis vormt voor de verkeersmonitoring. Een voorbeeld van een normatieve standaard is het tellen van toegang tot een database die persoonlijke gegevens bevat als een indicator die de naleving van privacy maatregelen bijhoudt.
De prestatie indicatoren moeten actief worden gemonitord en in real-time worden weergegeven. Deze 'bewakingstaak' moet vallen onder de verantwoordelijkheid van de verantwoordelijke operationele afdeling, die ook relevante stakeholders moet informeren als de prestaties van het systeem de aanvaardbare drempels overschrijden of onvoldoende zijn.

5.4 Beperkte bekendheid van de Digitale Gracht bij vaarweggebruikers

Niet alle gebruikers van de Amsterdamse vaarwegen lijken op de hoogte te zijn van de Digitale Gracht, en zelfs als ze dat wel zijn, hebben ze een beperkt begrip van het functioneren van het systeem. Momenteel wordt een enigszins verouderd overzicht van de sensoren die gebruikt worden en hun locatie verstrekt in het Amsterdamse sensorenregister (stand van zaken van de sensoren in 2022). De gebruikte algoritmen worden op hoofdlijnen beschreven in het algoritmeregister (het team Digitale Gracht heeft vastgesteld dat beschrijvingen gedetailleerder worden bijgewerkt voordat een algoritme met een hoog risico wordt ingezet). Daarnaast worden vaartuigeigenaren bij de aankoop van een vignet per brief verwezen naar een video op de website van de gemeente waarin het gebruik van de chips die aanwezig zijn in de vignetten voor verkeersmonitoring wordt genoemd. Deze bronnen leggen het functioneren van het systeem op een begrijpelijke manier uit. De meeste mensen zijn echter niet op de hoogte van het bestaan van deze bronnen. We zijn van mening dat de gemeente beter moet presteren in het vergroten van het bewustzijn over dit systeem bij het publiek. Vaartuigeigenaren krijgen te weinig informatie over het systeem. Op het moment van monitoring beperkt de beschikbare informatie zich tot een sticker die naar onze mening onvoldoende informatie biedt over de sensor en in veel gevallen nauwelijks leesbaar is voor iemand die per boot reist.

Het faciliteren van een functionele democratische discussie over 'smart city' systemen binnen de samenleving van Amsterdamse vereist een bepaald niveau van bewustzijn bij burgers en begrip van technische systemen. Het ontbreken van deze informatie staat haaks op de ambities van de stad met betrekking tot transparantie in slimme systemen, zoals deze geformuleerd zijn in de Tada-waarden (tada.city, 2017).

Naast bewustwording en informatie over de werking (algoritmeregister), richten we ons ook op de daadwerkelijke data die verzameld wordt door de Digitale Gracht. Hier kunnen we onderscheid maken tussen gegevens over de vaarweggebruikers zelf (wat heeft de stad over mij en mijn vaartuig verzameld?) evenals toegang tot de algehele data op geaggregeerd niveau (diepgaande maar geaggregeerde historische of actuele informatie over drukte). Momenteel kunnen waterweggebruikers geen gegevens vinden die over hen zijn verzameld, noch geaggregeerde gegevens verkrijgen.

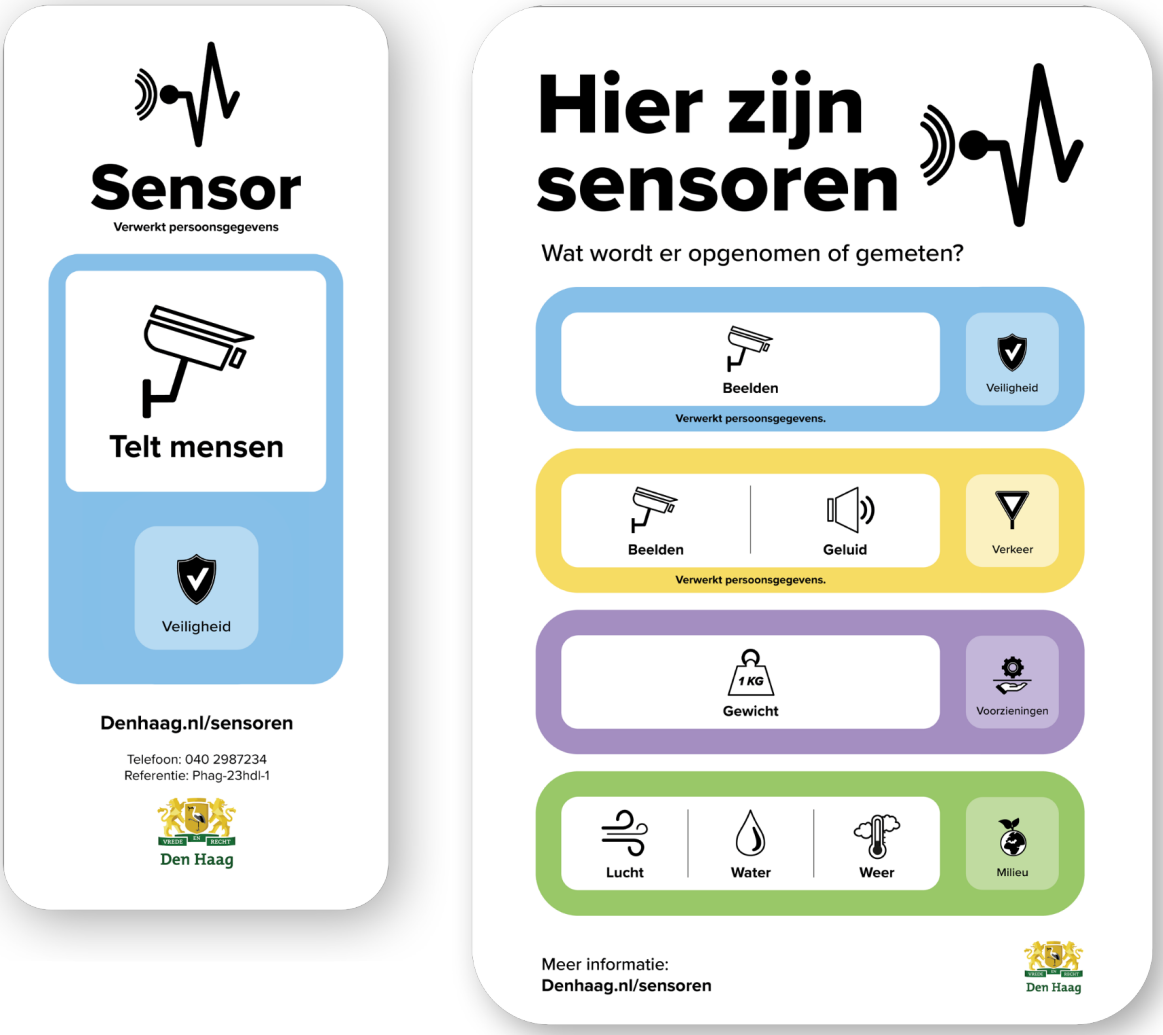
Geïnspireerd door:
- *Tada principe: Open en transparant, Van iedereen voor iedereen (tada.city, 2017).*

- *VNG Principes voor de Digitale Samenleving 2022, paragraaf 4.3. (Vereniging van Nederlandse Gemeenten, 2022).*
- *Amsterdamse Datastrategie, Data van de stad, voor de stad, p.19 (Gemeente Amsterdam, 2021).*

5.4.a Aanbeveling: Opzetten van proactieve publiekscommunicatie
Gemeente Amsterdam zou proactiever moeten zijn in het bewustmaken van het publiek van het bestaan van het systeem.

Om ervoor te zorgen dat het publiek geïnformeerd is over en betrokken wordt bij de werking van het systeem, moet de informatievoorziening bij de meetpunten worden bijgewerkt in overeenstemming met de “Landelijke communicatierichtlijn overheid sensoren in de publieke ruimte”. De borden bevatten een link naar andere bronnen (sensorenregister, algoritmeregister). Figuur 5 geeft hiervan een voorbeeld.

De transparantie van het systeem wordt vergroot door de verzamelde gegevens toegankelijk te maken op gevestigde contactpunten, waaronder het sensorenregister en/of het algoritmeregister. Om geaggregeerde gegevens toegankelijk te maken voor het publiek moet een speciale website worden ontwikkeld, die dient als platform voor het publiek om zowel live als historische gegevens te raadplegen. Bovendien moeten maatregelen worden genomen die individuele burgers in staat stellen te achterhalen wie toegang heeft (gehad) tot gegevens die betrekking hebben op henzelf of hun vaartuigen. Privacyrisico’s moeten worden aangepakt door het abstraheren van openbaar beschikbare gegevens met behulp van samenvattings-, groeperings- en verstoringstechnieken (Hoepman, 2022), gericht op het verminderen van het risico op heridentificatie bij het integreren van dashboardgegevens met persoonsgegevens, zoals opgenomen video's.



Figuur 5 - Voorbeeld van communicatierichtlijnen ontwikkeld in het project "Landelijke communicatierichtlijn overheidssensoren in de publieke ruimte". Rechts: voorbeeld van een sticker voor naast een camera. Links: voorbeeld van een bord met daarop de sensoren die in een gebied worden gebruikt. Meer gedetailleerde informatie over dit project is te vinden op responsiblesensinglab.org.

5.5 Onduidelijk beleid voor toegang tot gegevens

Toegang tot data wordt onvoldoende gestuurd door de rollen en verantwoordelijkheden van de persoon, en de gemeente lijkt onvoldoende overzicht te hebben van de samenhang tussen de data in de Digitale Gracht en het BHG controleproces. De toegangsrechten zijn grofweg gedefinieerd, wat inhoudt dat mensen toegang hebben tot gegevens die niet nodig zijn voor hun huidige rol. Bijvoorbeeld: op dit moment hebben alle gebruikers van het Digitale Gracht dashboard, waaronder Nautisch Beheer en het nautisch beleidsteam, realtime toegang tot de individuele hardwarenummers van particuliere vaartuigen die zijn geregistreerd door de vaste RFID-sensoren. Wij beschouwen deze informatie echter als irrelevant voor hun verantwoordelijkheden. Onderzoekers hebben toegang tot ruwe gegevens die mogelijk niet essentieel zijn voor hun analyses. In het verleden hadden alle gebruikers van het Digitale Gracht dashboard toegang tot alle gegenereerde rapportages. Het Digitale Gracht-team heeft eerder al vastgesteld dat adequate toegangsbeheer een probleem is en heeft deze kwestie aangepakt door rapportagefuncties uit te schakelen totdat het toegangsbeheer is verbeterd.

Geïnspireerd door:

- *Tada principe: Legitimate and monitored (tada.city, 2017).*

5.5.a Aanbeveling: Beperk toegang tot data tot een 'need-to-know' basis
In het kader van het beheer van gegevenstoegang adviseren we om toegangsrechten standaard tijdelijk te maken en vervaldata op te nemen. Gebruikers moeten ook waarschuwingen ontvangen die aangeven wanneer hun toegang dreigt te verlopen. Om de privacy te waarborgen, moeten maatregelen worden genomen om ervoor te zorgen dat data-analisten geen toegang krijgen tot ruwe, niet-geanonimiseerde gegevens. Het gebruik van bijna-realtime gegevensweergaven wordt alleen aanbevolen wanneer dit absoluut noodzakelijk is; anders wordt het abstraheren van gegevens aangemoedigd voor verbeterde veiligheid. Met name de functionaliteit die wordt gebruikt om BOA's te sturen (d.w.z. informatiegestuurde handhaving) moet gebruikmaken van geabstraheerde gegevens om operationele behoeften in evenwicht te brengen met privacybelangen.
Hoewel autorisatie noodzakelijk is om de toegang tot gegevens te beperken tot een "need-to-know" basis, is het nog steeds noodzakelijk om het systeem te decentraliseren zoals beschreven in Aanbeveling 5.1.b zodat geen enkele partij te bepalend wordt in de ontwikkeling en werking ervan.

5.5.b Aanbeveling: Beperk de afhankelijkheid van de vignetadministratie
We blijven enigszins onzeker over het gebruik van de vignetadministratie voor toepassingen van de Digitale Gracht. Over het algemeen raden we aan om de afhankelijkheid van huidige of toekomstige Digitale Gracht-toepassingen van de vignetadministratie te elimineren of op zijn minst aanzienlijk te beperken vanwege zorgen over dataminimalisatie. Als bijvoorbeeld unieke elektronische kenmerken gekoppeld aan persoonsgegevens worden gebruikt om te controleren op betaling van BHG, moet worden gegarandeerd dat geen enkele andere toepassing, zoals verkeersmonitoring, gebruikmaakt van deze ID's. Dit vereist strenge controle over de toegang tot de vignetadministratiedatabase, waarbij deze zowel fysiek als logisch moet worden gescheiden van andere systemen, evenals de beperking van toegang tot gegevens op 'need-to-know'-basis, en het verwijderen van gegevens die niet door enig doel worden gebruikt. Dit is in lijn met het eerdere advies van de Commissie Persoonsgegevens Amsterdam (2020).

5.6 Informatiegestuurde handhaving

Het gebruik van gegevens om hotspots vast te stellen voor informatiegestuurde handhaving wordt door verschillende onderzoekers als problematisch beschouwd. Een fundamenteel bezwaar is dat mensen binnen hotspots meer onder toezicht staan dan mensen daarbuiten op basis van factoren waarvoor ze niet verantwoordelijk kunnen worden gehouden. In het geval van de Digitale Gracht is een hotspotbenadering voorgesteld voor controles op geluidsovertredingen en het opsporen van illegale passagiersvaart, evenals controles op snelheidsovertredingen of overtredingen bij het aanmeren van commerciële vaartuigen.

Wij zijn van mening dat een handhavingsaanpak die volledig is gebaseerd op informatie die is verzameld via een hotspotbenadering vanuit ethisch perspectief onwenselijk is. Vanuit praktisch oogpunt kan een op hotspot gebaseerde aanpak als gunstig worden beschouwd gezien de beperkte beschikbare handhavingscapaciteit. Het gebruik van een hotspotbenadering kan echter alleen worden gerechtvaardigd als het de efficiëntie aanzienlijk en aantoonbaar verhoogt ten opzichte van andere benaderingen.

5.6.a Aanbeveling: Maak niet alleen gebruik van data-gedreven prioritering van inzet van handhavers
Zorg voor een evenwicht tussen de hotspotbenadering en een rasterbenadering (willekeurige controles) tijdens de controles. De rasterbenadering moet helpen om de hotspots voortdurend

opnieuw te definiëren. Zo zijn de hotspots dynamisch en worden de locaties gerechtvaardigd door de rasterbenadering. Om de transparantie te behouden, moeten de hotspots bovendien publiek toegankelijk zijn, d.w.z. dat de informatie over de gebieden die aan hoger toezicht worden onderworpen, openbaar beschikbaar moet zijn.

Knelpunten en aanbevelingen voor specifieke doelstellingen

5.7 Overmatige gegevensverzameling voor verkeersmonitoring

Het verkeersoverzicht wordt voornamelijk gecreëerd door een systeem van RFID-sensoren die op strategische locaties zijn geplaatst en die de unieke hardwarenummers van RFID-vignetten van passerende vaartuigen scannen. Door de gegevens van de sensoren te combineren, kunnen de waarschijnlijke routes die vaartuigen hebben afgelegd tussen de sensoren worden afgeleid.

Het volgen van individuele vaartuigen voor verkeersmonitoring kan worden gedaan in overeenstemming met de Algemene Verordening Gegevensbescherming (AVG), maar brengt risico's met zich mee. Naast het voldoen aan de wettelijke vereisten, moet het systeem ook een perceptie van privacy bieden. Zo heeft het langzaam verkeer monitoringsysteem dat in het stadscentrum operationeel is (CSMA/LVMA) en wordt beheerd door V&OR (Verkeer en Openbare Ruimte) in Amsterdam, bijvoorbeeld ervoor gekozen om geen wifi-tracking te gebruiken voor het voetgangersverkeer vanwege de politieke en maatschappelijke gevoeligheden die gepaard gaan met tracking en de effecten daarvan op privacy.

De huidige aanpak van het detecteren en verwerken van de gegevens voor het schatten van het verkeer heeft de volgende potentiële problemen.
Ten eerste, hoewel we er niet vanuit kunnen gaan dat de eigenaar van het vaartuig altijd aan boord van het schip is (wat betekent dat de locatiegegevens van het schip mogelijk niet altijd als persoonsgegevens volgens de AVG worden aangemerkt), is het waarschijnlijk dat veel vaartuigen wel vaak hun eigenaar aan boord hebben. Het continu monitoren van vaartuigbewegingen kan tevens worden gezien als een mogelijke inbreuk op de privacy door zowel burgers als organisaties die opkomen voor digitale rechten.
Ten tweede worden de gegevens momenteel in ruwe vorm verwerkt en opgeslagen, waardoor ze gevoelig zijn voor beveiligingsinbreuken. In het geval van een beveiligingsincident kunnen de gegevens met betrekking tot de bewegingen van personen worden gecompromitteerd. Het is belangrijk op te merken dat een inbreuk op de beveiliging die zich beperkt tot gegevens van vignetdetecties (d.w.z. de hardwarenummers) niet automatisch de identificatie van individuen mogelijk maakt. Hiervoor is toegang tot de vignetadministratie nodig of moet het verkeerspatroon van een vignet duidelijk herleidbaar zijn tot een enkel vaartuig/eigenaar, hoewel het laatste scenario onwaarschijnlijk is.
Ten derde maakt de huidige aanpak van verkeersmonitoring het mogelijk dat BOA's van Nautisch Toezicht en Handhaving de database die wordt onderhouden door PortPay, die persoonlijke informatie over de eigenaar van het vaartuig (vignetadministratie), samenvoegen met de beschikbare gegevens op het dashboard om particuliere booteigenaren te monitoren. Het combineren van de twee databases maakt het mogelijk voor de BOA om de locatie en tijd van een individueel vaartuig te weten, samen met alle persoonlijk identificeerbare gegevens van de eigenaar. Wij geloven dat Nautisch Toezicht en Handhaving op dit moment geen intentie heeft om de databases te combineren, maar het systeem heeft op dit moment geen ingebouwde beveiligingsmaatregelen hiertegen.

Wij beschouwen het verzamelen van gegevens met betrekking tot commerciële vaartuigen als minder problematisch, want minder privacygevoelig. Er zijn echter gevallen waarin de gegevens van commerciële vaartuigen als persoonsgegevens kunnen worden beschouwd (bijvoorbeeld in het geval van een eenpersoonsbedrijf). In dergelijke gevallen moet voldoende zorgvuldigheid worden betracht bij het verzamelen van gegevens van commerciële vaartuigen. Uiteindelijk moet de beslissing om gegevens van commerciële vaartuigen voor beleidsdoeleinden te verzamelen in overleg met de rederijen worden genomen.

Geïnspireerd door:

- *VNG Principes voor de Digitale Samenleving 2022, paragraaf 7.5, dataminimalisatie (Vereniging van Nederlandse Gemeenten, 2022).*

5.7.a Aanbeveling: Streef naar dataminimalisatie tijdens verkeersmonitoring
We bevelen aan om een privacyvriendelijke aanpak te hanteren voor het monitoren van verkeer in de Digitale Gracht. Het type monitoring kan worden bepaald aan de hand van de acceptabele nauwkeurigheid. We stellen de volgende varianten van het systeem voor, van minst tot meest data-intensief:

Verkeersmonitoring op basis van tellingen
Het principe van dataminimalisatie vraagt erom dat alleen noodzakelijke gegevens worden verzameld. Wij zijn van mening dat het niet nodig is om informatie (RFID-nummer en locatie) over individuele vaartuigen te hebben om het verkeer in de grachten te schatten. Het weten van het aantal vaartuigen op afzonderlijke strategische locaties zou voldoende moeten zijn. Om een vergelijkbare nauwkeurigheid te bereiken, kan het nodig zijn om sensoren op meer locaties in te zetten. Een dergelijke strategie zou echter het gebruik van privacyvriendelijke waarnemingsmethoden mogelijk maken.

Het gebruik van radars zou bijvoorbeeld verder kunnen worden onderzocht. Uit onze interviews is gebleken dat de Digitale Gracht heeft geëxperimenteerd met het gebruik van radarsensoren, maar het onderzoek kon niet worden afgerond. Radartechnologieën zoals millimetergolf (mmWave) detecteren objecten als een cluster van punten (puntenwolken), waardoor “privacy by design” wordt gewaarborgd. Deze technologieën zijn getest op het analyseren van het wegverkeer en zouden ook kunnen werken voor het tellen van vaartuigen. Bovendien zou het gebruik van een telmethode die onafhankelijk is van vignetten helpen om de Digitale Gracht volledig te isoleren van BHG administratie, waardoor function creep verder zou worden vermeden.
In de huidige systemen worden camera's gebruikt als aanvullende sensoren ter bevestiging van het aantal dat geteld wordt door RFID-sensoren. Camera's leggen van nature het uiterlijk van personen vast, wat privacy risico’s oplevert waarvoor weer risicobeperkende maatregelen moeten worden genomen. Dat is extra werk, en vaak blijft na mitigatie een restrisico over. De voorkeur gaat uit naar de minst invasieve detectiemethode wanneer daarmee hetzelfde doel kan worden bereikt. Dit perspectief sluit aan bij de Amsterdamse Datastrategie die stelt dat mensen door stedelijke ruimtes moeten kunnen navigeren zonder constant te worden geobserveerd (Gemeente Amsterdam, 2021). Handmatige tellingen zouden kunnen gebruikt worden als middel om de nauwkeurigheid te valideren in plaats van camera's. Tellingen via handmatige controles op een paar locaties kunnen vergeleken worden met de tellingen via radarsensoren. Winnie Daamen, universitair hoofddocent aan de leerstoel ‘Traffic Operations and Management’ van de afdeling Transport & Planning aan de TU Delft, voert momenteel een analyse uit om het aantal locaties voor het implementeren van sensoren te optimaliseren. Het resultaat van deze analyse is de eerste stap naar de implementatie van deze suggestie.

Monitoringsysteem voor het tellen van vaartuigen en categorieën
Als het gebruik van vignetten moet worden voortgezet, kunnen alleen de afzonderlijke categorieën worden gelezen en verwerkt via de RFID-nummers. Individuele hardwarenummers, of het nu ruwe data is of geanonimiseerd, mogen niet worden geregistreerd, verwerkt, opgeslagen en weergegeven op het dashboard. Het systeem voor het ophalen van categorieën uit hardwarenummers moet onafhankelijk zijn van de vignetten database, zodat er geen persoonlijke informatie met betrekking tot vignetten kan worden opgehaald.

RFID tracking verkeersmonitoringssysteem
Deze alternatieve methode wordt alleen voorgesteld als het absoluut noodzakelijk is om de doorvaart van individuele vaartuigen te registreren. In dat geval kan het huidige systeem van het uitlezen van de individuele elektronische identificatie worden voortgezet.
Zelfs in dit geval raden we aan dat de identificatie niet in ruwe vorm wordt opgeslagen of weergegeven op het dashboard. Gegevens moeten vroeg in het proces gepseudonimiseerd worden. Alleen gepseudonimiseerde gegevens mogen zichtbaar zijn op het dashboard of beschikbaar worden gesteld tijdens de gegevensverwerking voor beleidsrapporten. Het opvragen van de onbewerkte elektronische ID's mag alleen in vooraf gedefinieerde situaties met goedkeuring van de data steward. Bovendien moeten in geval van toegang tot deze gegevens, de momenten worden gelogd met details zoals wie deze data heeft geraadpleegd, wanneer en met welk doel. Deze informatie moet ook aan de eigenaar van het vaartuig worden doorgegeven.

5.8 Proportionaliteit aanpak opsporing illegale passagiersvaart

De stad reguleert de commerciële passagiersvaart door middel van een vergunningsproces. Deze regulering wordt gehandhaafd door commerciële passagiersvaart zonder vergunning te beboeten. De boetes dienen ter handhaving van het verbod op passagiersvaart zonder vergunning.
In de praktijk houdt handhaving in dat BOA's verdachte vaartuigen op het water identificeren, deze aanhouden op het moment dat ze verdacht zijn, de schipper en de opvarenden ondervragen over de situatie en, in sommige gevallen, de schipper of eigenaar van het schip een boete of last onder dwangsom opleggen.
In de aanpak die bedacht is voor de Digitale Gracht wordt voor het identificeren van hotspots van verdachte vaartuigen gebruikgemaakt van een algoritme dat patronen in vaarbewegingen identificeert die kunnen wijzen op illegale passagiersvaart. Om dit te kunnen doen, worden alle verzamelde gegevens van vaarbewegingen van particuliere vaartuigen verwerkt. De gegevens worden verzameld met behulp van RFID-sensoren. Dit betekent dat een groot aantal vaartuigen dat zich niet bezighoudt met illegale passagiersvaart onder de loep wordt genomen. Critici van deze aanpak noemen dit ‘sleepnet surveillance’. Vanwege de aanzienlijke inbreuk op de privésfeer van schippers vereist de eis van proportionaliteit een ernstige rechtvaardiging. Wij vragen ons af of aan deze eis wordt voldaan.
Proportionaliteit is uiteindelijk een oordeel en hangt af van de positie van degenen die het oordeel vellen ten opzichte van de zaak waar het om gaat. Het heeft ook te maken met de effectiviteit van de middelen en de beschikbaarheid van minder ingrijpende middelen. Als een groep experts met een zekere mate van afstand tot het project, zijn wij van mening dat de doeleinden (het identificeren van hotspots van passagiersvaart zonder vergunning) het toegepaste middel (het volgen van alle vaarbewegingen) niet rechtvaardigen. Wij geloven dat het beperkt nut heeft en dat er minder ingrijpende middelen zijn om een vergelijkbaar doel te bereiken.

Een secundair gebruik voor de gegevens uit de rapportage is genoemd. De gegevens zouden mogelijk als bewijs kunnen dienen in het geval van een rechtszaak over de boete tussen de gemeente en de verdachte van commerciële scheepvaart zonder vergunning. De aanpak is echter nog niet gevalideerd en daarmee is de betrouwbaarheid van de rapportage onvoldoende.

5.8.a Aanbeveling: Heroverweeg aanpak opsporen illegale passagiersvaart
In plaats van het inzetten van een algoritme om hotspots van verdachte vaartuigen te identificeren door de vaarbewegingen van alle particuliere vaartuigen te monitoren, raden we aan om te vertrouwen op benaderingen die eerder in gebruik zijn geweest om illegale passagiersvaart op te sporen. Dit omvat het scannen van het internet op advertenties voor illegale passagiersvaarten en het inzetten van personeel om handmatig te controleren op illegale passagiersvaart met een passende frequentie en op locaties waar dergelijke incidenten zich kunnen voordoen en waar illegale vaart schade kan veroorzaken aan legale aanbieders door het wegkapen van klanten. De frequentie van de handmatige controles kan na evaluatie worden aangepast. Als in plaats daarvan wordt gekozen voor een aanpak op basis van de unieke elektronische identificatiemiddelen om de vaarbewegingen van particuliere vaartuigen te monitoren, moet de toegang tot deze gegevens strikt worden beperkt, zoals beschreven in aanbeveling 5.5.a Beperk gegevenstoegang op basis van de noodzaak om te weten. BOA's mogen niet worden voorzien van de unieke elektronische ID’s van de vaartuigen die als verdacht zijn aangemerkt, maar alleen van de locaties waar wordt vermoed dat overtredingen plaatsvinden.

5.9 Proportionaliteit aanpak van geluidsmonitoring

Tot voor kort zou de combinatie van het weergeven van het unieke hardwarenummer dat is geregistreerd door RFID-sensoren en van geluidsgebeurtenissen op specifieke meetpunten op het Digitale Gracht dashboard de gebruikers van het dashboard in staat hebben gesteld om individuele vaartuigen te identificeren die geluidshinder veroorzaken. We geloven dat deze informatie nooit is gebruikt voor handhaving, dat wil zeggen dat het geen invloed heeft gehad op beslissingen van BOA's, maar we beschouwen dit als een onnodig privacyrisico. Het koppelen van deze informatie is voor geen enkele toepassing vereist en het kan BOA's, die toegang hebben tot de database van de vignetadministratie, in staat om geluidsgebeurtenissen te koppelen aan de eigenaren van specifieke vaartuigen.

In het verleden is een toepassing getest die specifiek bedoeld was om individuele vaartuigen te identificeren die geluidsoverlast veroorzaakten. Hierbij werden video- en audio-opnamen gemaakt van het vaartuig waarvan dat werd geïdentificeerd als veroorzaker van geluidsoverlast. Het weten van de huidige locaties van vaartuigen die geluidshinder veroorzaken is echter niet voordelig voor het handhavingsproces, gezien de aanzienlijke tijd die nodig is voor handhavers om de locatie te bereiken. Dienstvaartuigen hanteren met dezelfde vaarsnelheid als andere boten, waardoor de ‘direct respons’ wordt verminderd. Vanwege hun lagere snelheid kunnen vaartuigen van Nautisch Toezicht en Handhaving het geïdentificeerde vaartuig niet makkelijk controleren en mogelijk bestraffen. Om deze redenen vinden wij dat het doel de middelen niet rechtvaardigt en dat de praktijk niet proportioneel is. Het opnemen van audio- en videomateriaal, vooral wanneer de gegevens niet bruikbaar zijn voor acties, schendt het principe van dataminimalisatie. In geval van een veiligheidsinbreuk brengt het verzamelen van overmatige gegevens de privacy van individuen in gevaar.

Geïnspireerd door:

- *Agenda Digitale Stad, Amsterdammers hebben het recht om niet bespied te worden tijdens het bewegen door de openbare ruimte (Gemeente Amsterdam, 2019).*

5.9.a Aanbeveling: Heroverweeg aanpak van geluidsmonitoring middels sensoren om geluidsoverlast te bestrijden
In elk geval adviseren we om af te zien van het maken van geluidsopnamen, omdat wij dit onevenredig vinden. Bovendien moet het onmogelijk worden gemaakt (of alleen mogelijk onder bepaalde vooraf bepaalde voorwaarden) om een individueel vaartuig te koppelen aan een

geluidsgebeurtenis. Dit betekent dat geluidsincidenten niet samen met unieke elektronische kenmerken op het dashboard kunnen worden weergegeven. Om de handhaving in goede banen te leiden, raden we aan om de huidige aanpak van Nautisch Toezicht en Handhaving aan te houden, die gericht is op het monitoren van “signalen”, waarbij “Signalen.Amsterdam” wordt gemonitord en BOA's worden ingezet naar hotspots, zonder het inbouwen van actieve geluidsoverlast-sensoren. Als er geluidsgegevens nodig zijn voor beleidsdoeleinden, moeten er geluidssensoren worden gebruikt die de privacy waarborgen (gebruik bijvoorbeeld dB-meters om het geluid op bepaalde punten te meten).

6. Mogelijke vervolgprojecten

6.1 Privacyvriendelijke detectiemethoden voor verkeersmonitoring
In overeenstemming met aanbeveling 5.7.a zijn we van mening dat de huidige strategie voor het monitoren van het verkeer van privévaartuigen, die sterk afhankelijk is van unieke elektronische identificatie en het afleiden van routes, niet in overeenstemming is met het principe van dataminimalisatie. We stellen een vervolgproject voor dat een alternatieve manier van verkeersmonitoring onderzoekt die privacyvriendelijke detectiemethoden omarmt. Radar technologieën, met name millimetergolf (mmWave), identificeren objecten als clusters van punten (puntenwolken), waardoor privacy by design wordt gewaarborgd. Het vervolgproject zou de haalbaarheid kunnen onderzoeken van het gebruik van mmWave-radars voor het observeren van het verkeer in de Gracht.

6.2 Optimalisatie van het metingsinterval - Balans tussen gegevensverzameling en privacy
Voortbouwend op de geoptimaliseerde sensorverdeling ontworpen door Dr. Winnie Daamen, zou een vervolgproject een alternatief kunnen verkennen waarbij sensoren niet constant gegevens verzamelen, maar alleen gedurende bepaalde, mogelijk willekeurige momenten. Het project zou de afweging tussen nauwkeurigheid van verkeersgegevens en dataminimalisatie onderzoeken, met als doel een ‘sweet spot’ te vinden, waarbij voldoende gegevens kunnen worden verzameld, zonder overdreven hoeveelheden.

6.3 Vergroten van publieke bewustzijn over de Digitale Gracht via informatievoorziening
Onze analyse concludeert dat de gemeente zou moeten streven naar meer transparantie en begrip met betrekking tot de Digitale Gracht. We stellen een vervolgproject voor dat tot doel heeft het publieke bewustzijn en de mate van betrokkenheid te vergroten op basis van een pilot waarin er getest wordt met informatievoorziening bij meetpunten in overeenstemming met de “Landelijke communicatierichtlijn overheid sensoren in de publieke ruimte”.

6.4 Bouwen aan burgerparticipatie in de ontwikkeling van de Digitale Gracht
Een vervolgproject gericht op het opzetten van een organisatie die kan dienen als vertegenwoordigend orgaan voor voortdurende controle van burgers (bijvoorbeeld in de vorm van een burgerraad) over het Digitale Gracht systeem. Het project zou tot doel kunnen hebben om voor te stellen wie zou moeten deelnemen, wat het handvest zou moeten zijn en hoe ze zouden moeten functioneren.

6.5 Monitoren van systeemprestaties met betrekking tot normatieve standaarden
Hoewel functionele doelstellingen momenteel worden gemonitord binnen de Digitale Gracht, is het opvallend dat het ontbreekt aan actieve monitoring van op publieke waarden gebaseerde standaarden. Een vervolgproject zou in detail kunnen onderzoeken hoe normatieve standaarden kunnen en moeten worden gemonitord en weergegeven in de context van de Digitale Gracht.

6.6 Naar een Amsterdams beleid voor ‘hotspotting’
De onderzoekers die we hebben geraadpleegd, beschouwen het gebruik van data om hotspots te creëren voor informatiegestuurde handhaving als problematisch. Een hotspotbenadering resulteert in een situatie waarin mensen binnen hotspots onder meer toezicht staan dan mensen die buiten de hotspots vallen, gebaseerd op factoren waarvoor zij niet verantwoordelijk kunnen worden gehouden. Tegelijkertijd zien we dat hotspotbenaderingen voor informatiegestuurde handhaving worden ingezet door verschillende overheidsinstanties die geloven dat dit de handhavings-efficiëntie zal verhogen. Een vervolgproject zou dit spanningsveld kunnen onderzoeken, met behulp van de context van de

Digitale Gracht als voorbeeld om te onderzoeken hoe we hiermee als stad/maatschappij moeten omgaan.

Referenties

- Alfrink, K., Keller, A. I., Kortuem, G. W., & Doorn, N. (2022). Contestable AI by Design: Towards a Framework. Minds and Machines: journal for artificial intelligence, philosophy and cognitive sciences. https://doi.org/10.1007/s11023-022-09611-z

- Bureau Telematica Binnenvaart, 2024. Convenant tussen het Ministerie van Verkeer en Waterstaat en Koninklijke Schuttevaer, Kantoor Binnenvaart, Centraal Bureau voor de Rijn- en Binnenvaart en de Vereniging van sleep- en duwbooteigenaren Rijn en IJssel. https://binnenvaart.org/wp-content/uploads/2009/08/convenant.pdf

- Commissie Persoonsgegevens Amsterdam. (2020). Advies digitale gracht 10 december 2020. https://www.amsterdam.nl/bestuur-organisatie/organisatie/overige/adviesraden/commissie-persoonsgegevens-amsterdam/adviezen-cpa-2020/advies-digitale-gracht-10-december-2020/#hae39d3ca-e06c-4fc3-8c39-8a959427bc38

- Gemeente Amsterdam. (2019). Agenda Digitale Stad. https://openresearch.amsterdam/nl/media/inline/2019/3/7/agenda_digitale_stad_versie_1_01_maart_2019.pdf

- Gemeente Amsterdam. (2021). City of Amsterdam Data Strategy. https://assets.amsterdam.nl/publish/pages/1017819/data_strategy_city_of_amsterdam_2021-2022.pdf

- Gemeente Amsterdam. (2023). Agenda Digitale Stad. https://assets.amsterdam.nl/publish/pages/964754/agenda_digitale_stad_2023_2026_wrt.pdf

- Hoepman, J.-H. (2022). Privacy design strategies. The little blue book. https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf

- Hubert, B. (2020, January 20). 5G: The outsourced elephant in the room. berthub. https://berthub.eu/articles/posts/5g-elephant-in-the-room/

- Hubert, B. (Interviewee) (2022, May 22). Waarom je nerdfluisteraars nodig hebt bij de overheid [Audio Podcast]. Stuurloos. De Volkskrant. https://omny.fm/shows/stuurloos/waarom-je-nerdfluisteraars-nodig-hebt-bij-de-overh

- Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy Artificial Intelligence. Government Information Quarterly, 37(3), Article 101493. https://doi.org/10.1016/j.giq.2020.101493

- Koops, B.-J. (2021). The concept of function creep. Law, Innovation and Technology, 13(1), 29-56. https://doi.org/10.1080/17579961.2021.1898299

- Tada.city. (2017). Het Tada Manifest. https://tada.city/

- Vereniging van Nederlandse Gemeenten. (2022). Principes voor de Digitale Samenleving. https://vng.nl/sites/default/files/2022-12/Principes-voor-de-Digitale-Samenleving.pdf

Bijlage

Bijlage 1: Vragenlijst

Onderstaand de vragenlijst geïnspireerd op de assessment toolkits IAMA , AIIA, DPIA en Plot4ai. Deze vragenlijst was leidend voor de verkenning van het Digitale Gracht systeem en de systemen ingezet voor het BHG betaalproces. De vragenlijst werd alleen gebruikt om inzicht te krijgen in de bovengenoemde systemen. Ze werden niet gebruikt voor het identificeren van problemen of aanbevelingen.

Original question(s)	**Source(s)**	**Category**	**Derived question for Digitale Gracht and BHG payment process**
What is the goal to be achieved with the deployment of the algorithm? What is the main goal here and what are subgoals? What is the purpose and intended outcome of the AI system? Describe the process and the (intended) processing activities and/or intended policies/regulations for which this DPIA is conducted. Give a brief description of the intended ai system (title, general description, problem statement, and domain)	IAMA, AIIA, DPIA	1. System version & Goals	**What are the goals of the system?**
	Own Question	1. System version & Goals	**What is the state of the system for which the questions are filled in? E.g. is it live, has it been prototyped, is it just an idea, etc.**
What type of algorithm will be used, or what type of algorithm will be developed? Why is this type of algorithm chosen?	IAMA	2. General description tech. system	**What type of sensors are being used in the system?**
What type of algorithm will be used, or what type of algorithm will be developed? Why is this type of algorithm chosen? Why is this type of algorithm chosen? Is there automated decision-making? If so, on what basis? Could our AI system automatically label or categorize people?	IAMA, DPIA, PLOT4ai	2. General description tech. system	**What type of processing is being used? Does the system rely on automated decision making in any way? If yes, explain. E.g. Does the system automatically label or categorize people?**
Location: where will deployment of the algorithm take place? Is it in a particular geographical area, is it with a particular group of people or files?	IAMA	2. General description tech. system	**Where is the system and its sensors deployed? How was the location chosen?**

What does the system architecture look like (how do the software components relate to each other)?	AIIA	2. General description tech. system	**What does the architecture of the system look like? I.e. what are the different components and parts and how do they relate to each other**
How can the AI system interact with other hardware or software (if applicable)?	AIIA	2. General description tech. system	**How can the system interact with other hardware or software (if applicable)? E.g. other sensors, boats, databases, etc.**
Are any specific hardware and software requirements documented?	AIIA	2. General description tech. system	**Are the hardware software requirements for the system documented? E.g. the camera must have a specific resolution for the system to work correctly.**
What type of data is going to be used as input for the algorithm, and from what sources is the data derived? Does the ai system handle personal data (does the AVG apply)? If yes, please complete the following questions also. If not, continue at 'relating to confidential data'. Indicate which (categories of) personal data are being processed?	IAMA, AIIA, DPIA	3. Data collection, Processing & Storage	**What type of data is collected as input for the system? E.g. categories of personal data, confidential data etc. For each type explain where this data comes from. E.g. sensors, databases etc.**
Is there any linking, enrichment or comparison of data from different sources?	DPIA	3. Data collection, Processing & Storage	**Is there any linking, enrichment or comparison of data from different sources?**
Are special personal data, criminal data and/or BSN also processed? If so, please indicate which data.	DPIA	3. Data collection, Processing & Storage	**Are special personal data, criminal data and/or BSN also processed? If so, please indicate which data.**
What are the purposes of the processing of personal data within the process?	DPIA	3. Data collection, Processing & Storage	**What are the purposes of processing personal data within the process?**
Will personal data be used for a purpose other than that for which it was collected?	DPIA	3. Data collection, Processing & Storage	**Will personal data be used for a purpose other than that for which it was collected?**

How is it ensured that the default settings of the relevant devices or applications are such that only the personal data necessary for the specific purpose is collected? Please indicate what measures have been taken.	DPIA	3. Data collection, Processing & Storage	**How is it ensured that the default settings of the relevant devices or applications are such that only the personal data necessary for the specific purpose is collected? Indicate what measures have been taken.**
Are personal data encrypted where possible?	DPIA	3. Data collection, Processing & Storage	**Is personal data encrypted where possible?**
Are personal data pseudonymised where possible?	DPIA	3. Data collection, Processing & Storage	**Are personal data pseudonymised where possible?**
Please indicate what alternatives have been considered to achieve the process in a way that is less intrusive in terms of impact on the privacy of data subjects?	DPIA	3. Data collection, Processing & Storage	**Please indicate what alternatives have been considered and which have been implemented to achieve the process in a way that is less intrusive in terms of impact on the privacy of data subjects?**
Describe the (categories of) data subjects whose personal data are being processed. Indicate whether vulnerable groups are involved.	DPIA	3. Data collection, Processing & Storage	**Describe the (categories of) data subjects whose personal data are being processed. Indicate whether vulnerable groups are involved.**
How many individuals' personal data are (approximately) processed as part of this process?	DPIA	3. Data collection, Processing & Storage	**How many individuals' personal data are (approximately) processed as part of this process? Name an amount in combination with an indication of time.**
How is personal or confidential data handled? (Consider the DPIA), How is the input(data) stored? Indicate on which data carrier the personal data is stored (hardware, software, networks)	AIIA, DPIA	3. Data collection, Processing & Storage	**How is the collected data handled /stored? Indicate also where it is stored. E.g. hardware, software, networks, etc.**
Is our data storage protected?	PLOT4ai	3. Data collection, Processing & Storage	**Is the data storage protected?**

Are we preventing Data Leakage?	PLOT4ai	3. Data collection, Processing & Storage	**What measures have been taken to prevent Data Leakage?**
Are personal data transferred to countries outside the European Union? If yes, please indicate which parties are involved and what safeguards are in place.	DPIA	3. Data collection, Processing & Storage	**Are personal data transferred to countries outside the European Union? If yes, indicate which parties are involved and what safeguards are in place.**
What is the retention period of the output(data)?, What is the retention period of the output(data)?, Have retention periods been identified? If yes, indicate what the retention periods are.	AIIA, DPIA	3. Data collection, Processing & Storage	**What is the retention period of each type of data?**
In what way is it realized that the data are actually deleted/anonymised?	DPIA	3. Data collection, Processing & Storage	**In what way is it realized that the data are actually deleted/ anonymised?**
If no retention periods are defined, are measures taken to delete the personal data nevertheless?	DPIA	3. Data collection, Processing & Storage	**If no retention periods are defined, are measures taken to delete the personal data nevertheless?**
Which internal and external responsible parties are involved in this process? Describe the division of roles within the set-up of the AI system (such as developer, client, project leader, management organizations and final manager). Which parties and individuals are involved in the development/use/maintenance of the algorithm?Who is the user of the AI system, who are the end users working with the system and which stakeholders are impacted by the AI system?	DPIA, AIIA, IAMA	4. Stakeholders, Roles & Responsibilities	**Which internal and external parties and individuals are involved in or impacted by the system? Consider the system's development, use and maintenance. What are their roles and responsibilities?**
Which people and/or groups were coordinated with when developing ai system? Have data subjects (or their representatives) been asked to give their views on the processing activities? Please indicate why yes/no. Indicate how the views of data subjects have been followed up. If this vision has not been followed up, explain why this has not been done.	AIIA, DPIA	4. Stakeholders, Roles & Responsibilities	**Which people, groups and/or organizations were coordinated with when developing the system? E.g. data subjects. How were their views followed up?**

Are we planning to use a third party AI tool?	PLOT4ai	4. Stakeholders, Roles & Responsibilities	**Are any third party tools / software used?**
If the algorithm was developed by an external party: have clear agreements been made about ownership and management of the algorithm? What are those agreements?	IAMA	4. Stakeholders, Roles & Responsibilities	**If the system or parts of it was developed by an external party: have clear agreements been made about ownership and management of the system? What are those agreements?**
Is access to the data controlled? Distinguish between input data and output data. Have all parties coming into contact with the personal data been identified?	IAMA, DPIA	4. Stakeholders, Roles & Responsibilities	**Who has access to what data? For what purpose do these individuals or groups have access to this data?**
Is access to the data controlled? Distinguish between input data and output data. Are access measures in place that allow only persons to access personal data to the extent necessary for the performance of their duties?	DPIA	4. Stakeholders, Roles & Responsibilities	**How is access to data controlled? Are access measures in place that allow only persons to access personal data to the extent necessary for the performance of their duties?**
	Own questions	4. Stakeholders, Roles & Responsibilities	**How is data, or insights derived from data, accessed? E.g. via dashboards, phone notifications etc.**
Through what procedures will decisions based on the algorithm be made?	IAMA	5. Influencing decision making procedures	**What decisions are influenced by the system? Who takes these decisions and how are these decisions influenced by the system? Feel free to mention examples.**
What role do humans play in making decisions based on the algorithm's output ('human in the loop') and how are they enabled to play that role? How is human control and supervision ensured?	IAMA, AIIA	5. Influencing decision making procedures	**What role do humans play in making decisions based on the system's output and how are they enabled to play that role?**
Will our AI system make automatic decisions without human intervention?	PLOT4ai	5. Influencing decision making procedures	**Does the system involve automatic decisions without human intervention?**

Are the personal data being used for another purpose that is not specifically defined?	DPIA	5. Influencing decision making procedures	**How is function creep avoided?**
To which individuals and groups inside and outside your own organisation is the operation of the algorithm made transparent, and how is this done? If personal data are collected directly from the data subject; what information is communicated at the time of collection? If the personal data are not collected directly from the data subject; what information is communicated at the time of collection (or at least within one month of being obtained)?	IAMA, DPIA	6. Communication & Consent	**To which individuals and groups inside and outside the Digitale Gracht is the system communicated to and its operation made transparent? For each of the individuals or groups, describe what is communicated to them as well as how and when this information is communicated.**
How are changes documented during the lifetime of the system?	AIIA	6. Communication & Consent	**How are changes during the lifetime of the system documented and communicated?**
	Own question	6. Communication & Consent	**Are the data subjects informed about who has access to their personal data?**
	Own question	6. Communication & Consent	**Are the data subjects informed about the retention periods of the sensed data?**
Is the consent given through a clear active act? If the processing activities are based on consent: is the consent freely, specifically, information-based and unambiguously given by the data subject?	DPIA	6. Communication & Consent	**Are the processing activities based on consent? If yes, describe how consent is given.**
Does the data subject have the possibility to withdraw consent at any time and without negative consequences?	DPIA	6. Communication & Consent	**Does the data subject have the possibility to withdraw consent at any time and without negative consequences?**

Are proper tools for evaluation, auditing and assurance of the algorithm provided?	IAMA	7. Scrutiny & Contestation	**What tools for evaluation, auditing and assurance of the system are provided? To whom?**
How is the output(data) tested (periodically) randomly and continuously for correctness?	AIIA	7. Scrutiny & Contestation	**How is the system or parts of it tested? What is tested? How often are these tests conducted? Who is responsible for the testing?**
How is the ai system monitored?	AIIA	7. Scrutiny & Contestation	**How is the system or its parts monitored? What is monitored? When are they monitored? Who is responsible for the monitoring?**
How is the ongoing accuracy of the system measured and ensured?	AIIA	7. Scrutiny & Contestation	**How is the ongoing accuracy of the system measured and ensured?**
In case of system failure, could users be adversely impacted?	PLOT4ai	7. Scrutiny & Contestation	**If the system is not working as intended, what plans are activated or actions taken?**
If a data subject wants to object, or file a complaint against a decision of the AI system, is it clear what steps they can take? The same applies to appeals. Do citizens have an effective possibility to lodge a complaint or object? Are mechanisms in place for end-users to make comments about the system (data, technology, target group, etc.)?	AIIA, IAMA	7. Scrutiny & Contestation	**Do citizens/stakeholders/data subjects have an effective possibility to comment or lodge a complaint or object? If so, in what way?**
Does the process take into account an effective exercise of the right to access?	DPIA	7. Scrutiny & Contestation	**Do the data subjects have the opportunity to access / review their personal data collected by the sensing systems?**

Are mechanisms in place for end-users to make comments about the system (data, technology, target group, etc.)? And how or when are these reports safeguarded (analyzed and tracked)? How is it ensured that comments from stakeholders and end-users are handled properly internally?	AIIA	7. Scrutiny & Contestation	**How is it ensured that comments, complaints or objections are handled properly internally?**
Are we protected from insider threats?	PLOT4ai	8. Known risks & Mitigation measures	**What threats with regards to this system is the Digitale Gracht team currently aware of? How is the system protected from them?**
Describe the measures proposed to mitigate the residual risk.	DPIA	8. Known risks & Mitigation measures	**Describe the measures proposed to mitigate the residual risk.**

Responsible Sensing Lab

Het Responsible Sensing Lab, een initiatief van gemeente Amsterdam en AMS Institute, onderzoekt hoe waarden als privacy, autonomie en transparantie kunnen worden geïntegreerd in het ontwerp van sensorsystemen in de publieke ruimte. Door middel van onderzoek, het ontwikkelen van prototypes en het uitvoeren van pilots levert het Lab een bijdrage aan een 'verantwoorde' slimme stad.

responsiblesensinglab.nl /responsible-sensing-lab

In samenwerking met

Gemeente Amsterdam