INFORMATIE
BEVEILIGINGS
DIENST

PIA VERSLAG

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN
VERENIGING VAN NEDERLANDSE GEMEENTEN

Inhoudsopgave

Inhoudsopgave **2**
1 Inleiding **3**
2 Privacy **6**
2.1 Het project 6
2.2 Management samenvatting 7
2.3 Eigenaarschap en verantwoordelijkheden 7
2.4 De gegevens 8
2.5 Betrokken partijen 8
2.6 Verzamelen van gegevens 8
2.7 Bewaren en vernietigen 8
2.8 Beveiliging 8
3 Impactanalyse **9**
3.1 Impact op de betrokkene 9
3.2 Risico onrechtmatige toegang 9
3.3 Risico ongewenste wijziging 10
3.4 Risico verdwijning gegevens 10
3.5 Impact op de organisatie 10
3.6 Impact van veranderingen op huidige plannen 10
4 Aanbevelingen **11**
4.1 Informeren van betrokkenen 11
4.2 Minimaal aantal gegevens verzamelen 11
4.3 Beperk de bewaartermijn 11
4.4 Beperken delen gegevens 12
4.5 Securitymaatregelen 12
4.6 Verwerkingsregister 12
4.7 Leverancier software en hardware 13
4.8 Gegevensbeschermingseffectbeoordeling 13
4.9 Voorafgaande raadpleging AP 13
4.10 Nieuwe DPIA bij veranderingen 13
Bijlage 1 - Criteria voor een aanvaardbare gegevensbeschermingseffectbeoordeling **14**

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

1 Inleiding

In het kader van het project ANPR (Automatic NumberPlate Recognition) is een PIA uitgevoerd.

Doel van deze rapportage

De rapportage kan worden gebruikt ten behoeve van:

- Discussie/gespreksfacilitatie
- Belangenafweging
- Advisering over aandachtspunten voor verdere ontwikkeling dan wel te nemen beveiligingsmaatregelen
- Faciliteren van besluitvorming

In de rapportage is ruimte voor de opdrachtgever om de uitkomsten en bevindingen van de PIA te bespreken. Er zijn door de opdrachtgever geen veranderingen doorgevoerd. De verspreiding van de PIA moet in het rapport expliciet worden benoemd. Deze rapportage is een nadere toelichting bij de vragenlijst PIA. Er zijn bevindingen gedaan die bij uitbreiding van de scope van het project tot aanvullende vragen kunnen leiden.

INFORMATIE
BEVEILIGINGS
DIENST

Privacy Impact Analyse Verslag

Gemeente Amsterdam

Afdeling: Assets

ANPR (Automatic NumberPlate Recognition)

Dienst: RVE Verkeer en Openbare Ruimte

Datum: 23-02-2018
Projectnummer: n.n.b.
Projectleider: [redacted]
Opdrachtgever: [redacted]
Versie: 0.9.4
Auteur: [redacted]
Functie: Privacy Specialisten PrivacyCompass
Validatie door: [redacted]
Functie: Privacy Officer Cluster Ruimte & Economie en Stadsdelen

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Versiebeheer

Versies

Versie	Datum	Auteur	Samenvatting van de wijzigingen
0.8	26-01-2018	[redacted]	Eerste versie op basis van PIA ANPR v0.9
0.9	28-01-2018	[redacted]	Review op basis van PIA ANPR v0.9
0.9.1	30-01-2018	[redacted]	Aanpassing PIA verslag ANPR n.a.v. meeting en verzoek betrokkenen van 29-01-2018
0.9.2	22-02-2018	[redacted]	Feedback opdrachtgever verwerkt
0.9.4	23-02-2018	[redacted]	Review feedback en aanvulling op verslag na telefonisch overleg met [redacted] d.d. 23-02-2018

Goedkeuring

Versie	Datum	Naam
0.9	29-01-2018	[redacted], Privacy Officer Cluster Ruimte & Economie en Stadsdelen
0.9.2	04-02-2018	[redacted]
	07-02-2018	[redacted] Projectmanager Milieuzone
0.9.4	23-02-2018	[redacted]
0.9.5	01-03-2018	[redacted]
0.9.5		[redacted], CISO

Ter informatie aan

Versie	Datum	Naam
1.0	28-02-2018	[redacted]
		[redacted], CIO

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

2 Privacy

2.1 Het project

De Gemeente Amsterdam is voornemens een systeem op te bouwen waarvoor er een aanbesteding wordt gedaan. Het zogehete ANPR-systeem (Automatic NumberPlate Recognition) bevat camera's en computersystemen waardoor informatieuitwisseling mogelijk wordt. De camera's worden voor voor verschillende toepassingen ingezet. Voor dit rapport wordt, gelet op de vraagstelling, primair uitgegaan van het doel handhaving van verkeersbesluiten voor de milieuzone Amsterdam, en subsidiair de daarmee verenigbare doelstellingen verkeersmanagement en verkeersonderzoek. Het reeds bestaande ANPR-camera systeem zal hiermee worden vervangen, uitgebreid en geoptimaliseerd.

Scope PIA

De scope van de PIA beperkt zich tot de ANPR-camera's en de ANPR Server uit onderstaande systeemplaat. De overige onderdelen van het systeem vallen buiten beschouwing van deze PIA. Deze scope is afgestemd met [redacted] en [redacted]. Er wordt vanuit gegaan dat derden geen toegang krijgen tot de gegevens op de ANPR-camera's en de ANPR Server anders dan nu al het geval is voor het realiseren van een procesverbaal bij overtreding van de milieuzone.

[redacted]

2.2 Management samenvatting

De voorgestelde verwerking van persoonsgegevens behelst het grootschalig monitoren van de bewegingen van alle burgers. De Algemene Verordening Gegevensbescherming (AVG) kent aan dit soort verwerkingen een bijzondere status toe. Het verwerken van persoonsgegevens voor het handhaven van een milieuzone, zoals nu gebeurt, is vanuit de AVG denkbaar. De grondslag voor de verwerking is milieubeleid met het oogmerk om de uitstoot van schadelijke uitlaatgassen, zoals fijnstof, te verminderen, dit ter verbetering van de lokale luchtkwaliteit. Het bestuur voert daarmee een taak van algemeen belang/openbaar gezag uit.

Om dit rechtmatig te doen, mogen gegevens niet langer worden bewaard dan strikt noodzakelijk is en moet de betrokkene erop kunnen vertrouwen dat deze gegevens ook alleen voor dit doel worden bewaard. Daarbij moet de inzet van de middelen goed worden gecommuniceerd middels bijvoorbeeld de website van de gemeente en borden boven de weg. Ook zal voor de beveiliging een goede risicoafweging noodzakelijk zijn. De gekozen en geldende norm, Baseline Informatiebeveiliging Gemeenten (BIG), is daarbij een goed startpunt.

Met de ketenpartners, het CJIB en eventueel de RDW, is het advies om in het geval van een relatie van Verwerkingsverantwoordelijke tot Verwerkingsverantwoordelijke e.e.a. vast te leggen in een overeenkomst. De relatie tussen Verwerkingsverantwoordelijke en Verwerker moet van rechtswege in een Verwerkersovereenkomst worden vastgelegd.

Wanneer de vernieuwing niet langer beperkt blijft tot het vervangen van de camera's met de bijbehorende servers, maar ook naar een andere architectuur gaan of de gegevens naar andere partijen worden doorgegeven zal een nieuwe DPIA over het systeem als geheel noodzakelijk zijn. In die fase zal het betrekken van alle stakeholders (dus ook met betrokkenen) onvermijdelijk worden.

2.3 Eigenaarschap en verantwoordelijkheden

Het college van B&W is eindverantwoordelijke voor het ANPR. Zij bepalen doel en middelen van de verwerking. Daarmee zijn zij aan te merken als Verwerkingsverantwoordelijke in de zin van de Algemene Verordening Gegevensbescherming.

De Wethouder Duurzaamheid heeft luchtkwaliteit in zijn portefeuille. De intern verantwoordelijke voor de gegevensverwerking ANPR is de directeur van de rve Verkeer en Openbare Ruimte, waarbij de proceseigenaar, de heer [redacted] als 'eigenaar' optreedt en de projectleider ANPR, de heer [redacted] als contactpersoon moet worden gezien. De rve Toezicht en Handhaving is verantwoordelijk voor operationale zaken. Aangezien dit een bestuursorgaan betreft is dit een interne relatie. Die is vanuit de AVG niet verder relevant. De Verwerkingsverantwoordelijke draagt de verantwoordelijkheid.

Tijdens gesprekken voor de PIA bleek het beeld te bestaan dat het eigenaarschap van de camera bepalend zou zijn voor de vraag wie Verwerkingsverantwoordelijke is. Echter voor de AVG is bepalend wie het doel en de middelen van de verwerking bepalen. In dit geval is dat evident, de gemeente die de eisen bijvoorbeeld ook in een aanbesteding neerlegt, het register van verwerkingen bijhoudt en het beleid uitvoert. Deze verantwoordelijkheid delen door camera's te

leasen (dus niet in eigendom te nemen) of door een ander bestuursorgaan te laten mee betalen verandert hier niets aan.

2.4 De gegevens

Technisch gesproken maakt het ANPR-systeem beelden d.m.v. inzet van camera's. Deze camera's kunnen een deel van de verwerking zelf regelen (bijvoorbeeld een kenteken op een vrachtauto, taxi, auto of brommer herkennen).

Indien verwerking niet mogelijk is door een te grote toevoer aan gegevens kan deze verwerking deels plaatsvinden op de ANPR-server waarmee de camera's verbonden zijn.

2.5 Betrokken partijen

De leverancier van de ANPR-camera's en ANPR Server is nog niet bekend. Bij het uitvoeren van de PIA is ervan uitgegaan dat er sprake is van uitbesteding van de levering van software en hardware aan leveranciers die zich aan een met Nederland vergelijkbare privacywetgeving moet houden.

De gegevens worden verstrekt aan CJIB en [redacted]:

1. CJIB heeft de kentekens nodig om boetes naar aanleiding van overtredingen van de milieuzones te kunnen versturen.
2. In het kader van deze privacytoetsing zijn er geen andere doelen denkbaar voor het verwerken van de persoonsgegevens door [redacted] dan het handhavend optreden binnen de milieuzones naar voertuigen die daar niet mogen komen.
3. Er zijn geen andere afnemers van het systeem. Binnen deze PIA is niet voorzien dat de Nationale Politie toegang krijgt tot de gegevens op de ANPR-camera's en de ANPR Server.

2.6 Verzamelen van gegevens

Er wordt een beperkte hoeveelheid gegevens verzameld voor een goede vervulling van de publieksrechtelijke taak: Een kwalitatief hoogwaardige openbare ruimte d.m.v. vergunning en/of ontheffing (in het kader van milieubeleid).

2.7 Bewaren en vernietigen

De maximale opslagcapaciteit van de ANPR-camera bedraagt maximaal 3 dagen en van de ANPR Server maximaal 28 dagen. De opslagcapaciteit is instelbaar. Na ingestelde periode worden de gegevens van de ANPR-camera en ANPR Server verwijderd. De gegevens moeten worden verwijderd op het moment dat zij niet meer ter zake dienend zijn. Zodra [redacted] voldoende informatie heeft om handhavend op te te treden, is er geen doel meer voor het langer bewaren van de gegevens. Het is dan ook de aanbeveiling om daarna de informatie op de server te verwijderen.

2.8 Beveiliging

Op basis van de VRA (Verkorte Risico Analyse) en de resulterende BIV-classificatie is bepaald dat de maatregelen uit de BIG (Baseline Informatiebeveiliging Nederlandse Gemeenten) voldoende zijn als deze baseline correct en zo volledig mogelijk wordt gevolgd.

De leverancier van de software en hardware zal mede geselecteerd worden gebaseerd op de mate van voldoen aan de securitymaatregelen.

3 Impactanalyse

3.1 Impact op de betrokkene

- Er wordt gebruik gemaakt van bestaande technologie (ANPR-camera's) én het verzamelen van meer of andere persoonsgegevens dan voorheen die bij het publiek vragen of weerstand op kan roepen.
- Er worden borden geplaatst die waarschuwen voor de handhaving van de milieuzones d.m.v. opnames met (ANPR-)camera's.
  Er worden meer gegevens verzameld dan noodzakelijk voor het doel van de verwerking (handhaving verkeersbesluit). Voor het doel van de verwerking zijn alleen de kentekengegevens en overtredingsfoto's nodig.
- Ook worden opnames gemaakt van voertuigen en personen die geen overtreding van de milieuzone begaan (waarbij men spreekt over passages).
- De gegevens worden aan [redacted]control verstrekt. Deze gegevens kunnen alleen dienen voor de handhaving van de milieuzone(s).
- Er worden geen profielen van de individuele betrokkenen of passanten opgesteld.

3.2 Risico onrechtmatige toegang

De kans op onrechtmatige toegang tot de gegevens is laag: De leverancier van de ANPR-camera's en de ANPR server wordt mede geselecteerd op basis van de mate van voldoen aan de securitymaatregelen uit de BIG (Baseline Informatiebeveiliging Nederlandse Gemeenten), die op basis van de BIV-classificatie voor het project van toepassing zijn (zie ook PvE ANPR). Ook is nadrukkelijk besloten zelf het beheer over de systemen en de applicaties te voeren. Door dit in 'eigen huis' te houden, is er betere regie mogelijk. De risico-inschatting kan veranderen indien dit beheer door een andere partij wordt uitgevoerd.

De schade bij onrechtmatige toegang van de gegevens is beperkt: er zou nagegaan kunnen worden welke voertuigen op een bepaalde datum en tijdstip op een bepaalde locatie waren. Het is echter niet mogelijk om vast te stellen welke persoon in een bepaald voertuig reed.

Tijdens de gesprekken kwam naar voren dat in het verleden is gekeken naar het gezamenlijk gebruik van dezelfde camera door meerdere bestuursorganen. Dit zou bijvoorbeeld de Politie kunnen zijn. In het tijdperk van een analoge camera wordt dit technisch gerealiseerd door het splitsen van het signaal en twee uitgangen te realiseren: een naar de gemeente en een naar de politie. Een dergelijke manier van benaderen is bij digitale camera's niet mogelijk. Een camera is door de digitalisering een geautomatiseerd werk. Zo is bijvoorbeeld een van de eisen dat beelden kunnen worden opgeslagen gedurende maximaal drie dagen om ze later op te halen. Dat opslaan en reproduceren is reeds een verwerking. Het doorgeven van de beelden aan een ander bestuursorgaan zou reeds het concept veranderen en daarbij ook nopen tot een nieuwe DPIA. Het doel van de verwerking en mogelijk ook de grondslag van de verwerking veranderen in een dergelijke situatie. Het is niet onwaarschijnlijk dat die toegang onrechtmatig zou zijn.

Het aansluiten van een dergelijk geautomatiseerd werk op twee netwerken verandert ook het beveiligingsmodel. Er is in zo'n geval sprake van een achterdeur op het industriele netwerk [redacted] van de Gemeente Amsterdam. Dit komt doordat de camera in zo'n geval verbonden zou zijn met twee netwerken: een van de gemeente en een van de gemeente Amsterdam. Door deze

netwerken met elkaar te verbinden met diverse camera's als verbindende factor. Hierdoor is het mogelijk of denkbaar dat via het netwerk van de politie wordt ingebroken op het netwerk van Amsterdam of omgekeerd. Daarbij komt de vraag op of een gemeente, die volgens andere normen beveiliging regelt dan de politie er niet tegenstellingen ontstaan. Ook is het maar zeer de vraag of de gemeente dan niet meer van het netwerk extra zal moeten beveiligen. Daarnaast zullen er dan afspraken over verantwoordelijkheid moeten worden gemaakt. Zo'n complexe situatie maakt een nieuwe risicoinschatting en een nieuwe gegevenseffectbeoordeling of PIA onvermijdelijk.

3.3 Risico ongewenste wijziging

De kans op ongewenste wijziging van de gegevens is laag: Er moet eerst onrechtmatige toegang tot de gegevens verkregen worden (zie: 3.2 Risico ongewenste wijziging).

De schade bij ongewenste wijziging van de gegevens is beperkt: er zou gesimuleerd kunnen worden dat bepaalde voertuigen op een bepaalde datum en tijdstip **niet** op een bepaalde locatie waren in een bepaald voertuig. Dit aangezien een ongewenste wijziging naar verwachting vooral betrekking zal hebben op het verwijderen van gegevens. Hiermee zouden overtreders van de milieuzones een boete kunnen ontlopen.

3.4 Risico verdwijning gegevens

Zie 3.3 Risico ongewenste wijziging.

3.5 Impact op de organisatie

Mochten er problemen onstaan op het gebied van beschikbaarheid, integriteit en betrouwbaarheid van de gegevens, dan hebben die geen impact op beleidsbeslssingen. Problemen op dit gebied kunnen wel leiden tot foutieve operationele beslissingen, maar die kunnen en zullen snel hersteld worden, en leiden niet of nauwelijks tot schade.

3.6 Impact van veranderingen op huidige plannen

De scope van de PIA is nu beperkt tot het aanschaffen van nieuwe camera's, een server-systeem met aansluiting op de reeds bestaande architectuur. Veranderingen die technisch ogenschijnlijk klein lijken, zoals het verlenen van toegang tot de camera aan derden via een netwerk of via een achterdeur in de camera, is vanuit de AVG iets wat juist een groot risico met zich meebrengt.

Het leveren van toegang tot de camera geeft een beheerslast voor de gemeente (de leveringsverplichting). Dat draagt het risico dat de gemeente opeens niet alleen Verwerkingsverantwoordelijke in de zin van de AVG is, maar ook Verwerker. Dat laatste betekent dat de AVG verplicht tot aansturing naar de Gemeente toe. Het doorleveren via een netwerk brengt de grondslag en doelbinding in gevaar.

4 Aanbevelingen

Naar aanleiding van de gegeven antwoorden op de vragen uit de PIA-vragenlijst en op basis van de 'Criteria voor een aanvaardbare gegevensbeschermingseffectbeoordeling' uit de 'Richtsnoeren voor gegevensbeschermingseffectbeoordelingen (in de zin van Verordening 2016/679)' van de Groep Gegevensbescherming Artikel 29 (zie: Bijlage 1 – Criteria voor een aanvaardbare gegevensbeschermingseffectbeoordeling) worden een aantal aanbevelingen gedaan.

Indien de aanbevelingen worden opgevolgd kan, uitgaand van de door Autoriteit Persoonsgegevens bekendgemaakte criteria, worden aangenomen dat het ANPR-systeem voldoet aan de eisen van de AVG en dat er is voorzien in toereikende waarborgen.

4.1 Informeren van betrokkenen

De betrokkenen moeten worden geïnformeerd over de gegevensverwerking. Dit moet op beknopte en begrijpelijke, en in gemakkelijk toegankelijk vorm, worden gedaan (art. 12 AVG).

Het is aan te bevelen om deze informatie op een website beschikbaar te stellen en hier naartoe te verwijzen vanaf de borden die waarschuwen voor de handhaving van de milieuzones d.m.v. opnames met ANPR-camera's. Plannen om borden toe te voegen bij plaatsing van de ANPR-camera's zijn al uitgevoerd.

4.2 Minimaal aantal gegevens verzamelen

Voor het handhaven van de milieuzones hoeven alleen kentekens en overtredingsfoto's verzameld te worden.

Bij de selectie van de ANPR-camera's en ANPR-server is het aan te bevelen om als selectiecriterium mee te nemen dat personen onherkenbaar in beeld worden gebracht en enkel het kenteken wordt vastgelegd.

Het is aan te bevelen gegevens te verwijderen op het moment dat is vastgesteld dat er geen sprake is van een overtreding. Voor het langer bewaren van de gegevens is immers geen grondslag binnen de vraagstelling. Ook zullen de gegevens van de server moeten worden verwijderd als er wel sprake is van een overtreding op het moment dat deze gegevens niet meer noodzakelijk zijn. Zodra [redacted] beschikt over voldoende informatie om handhavend op te treden en de rechtsgang (b
ezwaar en beroep) te borgen, valt niet in te zien waarom gegevens langer bewaard mogen blijven.

4.3 Beperk de bewaartermijn

Beperk de bewaartermijn tot het maximaal noodzakelijke.

Voor de ANPR-camera's is dat de maximale tijd van opname door de ANPR-camera tot doorgifte aan de ANPR-server.

Voor de ANPR-server is dat de maximale tijd van opname door de ANPR-camera tot doorgifte aan [redacted] en zij beschikken over voldoende informatie om handhavend op te treden en de rechtsgang (bezwaar en beroep) te borgen.

4.4 Beperken delen gegevens

De primaire grondslag is het uitvoeren van beleid gericht op het terugdringen van schadelijke emissies van voornamelijk fijnstof. Dit beleid heeft betrekking op milieubeleid, zoals bedoeld in de Wet milieubeheer en raakt dan ook artikel 2 EVRM (het recht op leven). Om te kunnen handhaven is het vaststellen dat een voertuig zich gemotoriseerd beweegt in de milieuzone noodzakelijk. Een camera kan dit geautomatiseerd doen. Voor het goed doorstromen van het verkeer kunnen beelden worden bekeken en ook statistieken worden bijgehouden van de tijd dat een voertuig zich in milieuzone bevindt. Gepseudonimiseerde gegevens worden opgeslagen in een systeem teneinde latere analyses van verkeersdruk mogelijk te maken en daarmee ook een betere doorstroming van het verkeer te waarborgen.

Bij geconstateerde overtreding zullen er noodzakelijke gegevens gedeeld worden met het CJIB. Het betreft hier dan kenteken, fotomateriaal, voertuig, plaats en tijdstip. De beschikbare data kan dus in afgeslankt bestand (art. 2 lid 1 AVG) worden gedeeld.

Er worden ook gegevens gedeeld met City Control. City Control kan voor het gebruik van deze gegevens alleen het doel waarvoor de gegevens zijn verzameld (milieuhandhaving). Zouden zij dat voor andere doeleinden gebruiken dan is daar geen grondslag voor. De gegevensverwerking wordt dan onrechtmatig.

Het delen van gegevens en/of data afkomstig uit het ANPR-systeem, al dan niet in afgeslankt bestand, mag alleen ten einde voor het handhaven van verkeersbesluiten (zoals handhaving milieuzones) of daarmee verenigbare doelstellingen in de vorm van verkeersmanagement en verkeersonderzoek. Voor andere doeleinden is geen grondslag.

4.5 Securitymaatregelen

Selecteer de leverancier van de ANPR-camera's en ANPR Server mede op basis van de securitymaatregelen uit de BIG (Baseline Informatiebeveiliging Nederlandse Gemeenten), die op basis van de BIV-classificatie voor het project van toepassing zijn.

Wij bevelen aan om te toetsen of de leverancier van de software én hardware zelf aan de securitymaatregelen voldoen. Bijvoorbeeld door het vereisen van een ISAE 3402 Type II certificering (internationaal erkende assurance standaard voor outsourcing) van de leverancier, de BIG. Om de beveiliging te verhogen kan bij softwareontwikkeling het gebruik van de Grip op SSD-methodiek nuttig zijn als vereiste. De Gemeente Amsterdam is aangesloten bij de Centrum voor Informatiebeveiliging en Privacybescherming om daar ondersteuning te vragen. De methodiek is risicogebaseerd en schept veel duidelijk tijdens het inkooptraject en de realisatie. Ook kan het een idee zijn om bij de inkoopvoorwaarden mee te nemen dat de koop pas wordt geaccepteerd na een penetratietest, het analyseren van de broncode of het uitvoeren netwerkanalyses. Met zo'n stap kan de leverancier een kans krijgen de manco's te verbeteren en de kwaliteit te verbeteren. Hiermee verkleint de gemeente het risico op slechte kwaliteitproducten met allerhanden risico's die vanuit de AVG gezien de verwerking onrechtmatig zouden maken.

4.6 Verwerkingsregister

Neem de verwerking, het registreren van kentekens ten behoeve van handhaving van milieuzones, op in het verwerkingsregister van de Gemeente Amsterdam.

4.7 Leverancier software en hardware

Maak gebruik van de GIBIT Amsterdam en stel een verwerkersovereenkomst op met de leverancier van de ANPR-camera's en ANPR-server.

4.8 Gegevensbeschermingseffectbeoordeling

De scope van deze Privacy Impact Assessment beperkt zich tot de ANPR-camera's en de ANPR-server. Het ANPR-systeem bevat echter nog meer componenten (zoals een ESB), derde partijen, gegevensverwerkingen.

Het is aan te bevelen om voor deze componenten eveneens een Privacy Impact Assessments uit te voeren om de privacyrisico's voor alle betrokkenen te waarborgen.

Voer ook opnieuw een Privacy Impact Assessment uit zodra men voornemens is om het ANPR uit te breiden met andere functionaliteiten of het aansluiten van andere gegevensbronnen, etc.

4.9 Voorafgaande raadpleging AP

Het vooraf raadplegen van de Autoriteit Persoonsgegevens zal niet leiden tot een vrijbrief. Deze route is gelet op het vervangen van camera's niet een noodzakelijke stap. Wanneer echter er AVG-technisch wezenlijke veranderingen optreden (bijvoorbeeld bij het spreken over doorgifte aan andere bestuursorganen, veranderingen in de doelstelling) kan dit nuttig zijn. Een zienswijze van de AP op voorhand voorkomt dan dat in een later stadium een last onder dwangsom de werking van het totale systeem ernstig zou gaan verstoren.

4.10 Nieuwe DPIA bij veranderingen

Het volgen van burgers en het bijhouden van registraties is zowel vanuit de AVG als de publieke perceptie gezien een gevoelige kwestie. Het anders inzetten van de systemen of het treffen van voorbereidingen daartoe kan leiden tot verwarring. Wanneer een nieuwe situatie ontstaat is een DPIA vanuit de AVG onvermijdelijk. Het betrekken van de betrokkenen (diegene die worden geregistreerd) is dan onvermijdelijk.

Bijlage 1 - Criteria voor een aanvaardbare gegevensbeschermingseffectbeoordeling

De WP29 stelt de volgende criteria voor die verwerkingsverantwoordelijken kunnen gebruiken om te beoordelen of een gegevensbeschermingseffectbeoordeling, of een methode voor het uitvoeren van een gegevensbeschermingseffectbeoordeling, volledig genoeg is om aan de AVG te voldoen:

- Er wordt een systematische beschrijving van de verwerking verstrekt (artikel 35, lid 7, onder a):
  - Er wordt rekening gehouden met de aard, omvang, context en doelen van de verwerking (overweging 90) ☑
  - De persoonsgegevens, de ontvangers en de periode gedurende welke de persoonsgegevens worden bewaard worden geregistreerd ☑
  - Er wordt een functionele beschrijving van de verwerking verstrekt ☑
  - De activa waarop persoonsgegevens steunen (hardware, software, netwerken, mensen, papier of papiertransmissiekanalen) worden geïdentificeerd ☑
  - Er wordt rekening gehouden met de naleving van de goedgekeurde gedragscodes (artikel 35, lid 8) n.t.b.
- De noodzaak en evenredigheid worden beoordeeld (artikel 35, lid 7, onder b):
  - De beoogde maatregelen om aan de verordening te voldoen worden bepaald (artikel35, lid 7, onder d), en overweging 90, waarbij rekening wordt gehouden met:
    - Maatregelen die bijdragen aan de evenredigheid en noodzaak van de verwerking op basis van:
      - Een of meer gespecificeerde, expliciete en legitieme doeleinden (artikel 5, lid 1, onder b)) ☑
      - Rechtmatigheid van de verwerking (artikel 6) ☑
      - Toereikend, ter zake dienend en beperkt tot wat noodzakelijke gegevens zijn (artikel 5, lid 1, onder c)) ☒ *Zie: 3.1 Impact op de betrokkene*
      - Beperkte bewaartermijn (artikel 5, lid 1, onder e)) ☑
    - Maatregelen die bijdragen aan de rechten van de betrokkenen:
      - Informatie verstrekt aan de betrokkene (artikelen 12, 13 en 14) ☒ *Zie: 4.1 Informeren van betrokkenen*
      - Recht van inzage en recht op overdraagbaarheid van gegevens (artikelen 15 en 20) ☒ *Zie: 4.1 Informeren van betrokkenen*
      - Recht op rectificatie en recht op gegevenswissing (artikelen 16, 17 en 19) ☒ *Zie: 4.1 Informeren van betrokkenen*
      - Recht van bezwaar en recht op beperking van de verwerking (artikelen 18, 19 en 21) ☒ *Zie: 4.1 Informeren van betrokkenen*
      - Relaties met verwerkers (artikel 28) ☒
      - Waarborgen omtrent internationale doorgifte(n) (hoofdstuk V) ☑
      - Voorafgaande raadpleging (artikel 36) ☒
- De risico's voor de rechten en vrijheden van betrokkenen worden beheerd (artikel 35, lid 7, onder c):
  - Er wordt rekening gehouden met de oorsprong, de aard, het specifieke karakter en de ernst van de risico's (zie overweging 84) of, meer specifiek, voor elk risico (onrechtmatige toegang, ongewenste wijziging en verdwijning van gegevens) vanuit het perspectief van de betrokkenen:

        - Er wordt rekening gehouden met de bronnen van de risico's (overweging 90) ☑
        - De mogelijke gevolgen voor de rechten en vrijheden van de betrokkenen worden geïdentificeerd in geval van gebeurtenissen zoals onrechtmatige toegang, ongewenste wijziging en verdwijning van gegevens ☑
        - Bedreigingen die kunnen leiden tot onrechtmatige toegang, ongewenste wijziging en de verdwijning van gegevens worden geïdentificeerd ☑
        - De waarschijnlijkheid en ernst worden ingeschat (overweging 90) ☑
        - De beoogde maatregelen om de risico's aan te pakken worden bepaald (artikel 35, lid 7, onder d), en overweging 90) ☑
- De belanghebbenden worden betrokken:
    - Het advies van de functionaris voor gegevensbescherming wordt ingewonnen (artikel 35, lid 2) ☑
    - Indien nodig wordt de betrokkenen of hun vertegenwoordigers naar hun mening gevraagd (artikel 35, lid 9) ☒

INFORMATIE BEVEILIGINGS DIENST

INFORMATIEBEVEILIGINGSDIENST
V00R GEMEENTEN (IBD)

NASSAULAAN 12
2514 JS DEN HAAG

POSTBUS 30435
2500 GK DEN HAAG

HELPDESK 070 373 80 11
ALGEMEEN 070 373 80 08
FAX 070 363 56 82

INFO@IBDGEMEENTEN.NL
WWW.IBDGEMEENTEN.NL

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN