ANPR-camera’s gebruiken voor analyses; Juridisch advies

Datum: 30 januari 2024
Auteurs: Sander Flight en Dimitri Pouwels

In opdracht van
Samenwerkingsproject Expertpool Stadslogistiek (SPES)
Ministerie van Infrastructuur en Waterstaat

Inhoud

Management samenvatting

Dit advies is bedoeld voor gemeenten die een zero emissie zone willen invoeren en deze willen handhaven met behulp van automatische kentekenherkenning. Om te zien of mensen zich houden aan de regels willen gemeenten vaak analyses uitvoeren op de database met gescande kentekens. Ze willen bijvoorbeeld zien hoeveel voertuigen een vrijstelling hadden. En waar voertuigen die de regels overtreden vandaan komen. Aan dat soort analyses zitten risico's vast voor de privacy van de betrokkenen. Het is niet zonder meer mogelijk om kentekens te gebruiken voor analyses. Maar onder bepaalde voorwaarden mag het wel degelijk. Dit advies biedt alle informatie die gemeenten nodig hebben om dit proces intern goed te organiseren.

In de meeste gemeenten met een toekomstige Zero Emissie-zone (ZE) wordt deze gehandhaafd met behulp van Automatic Number Plate Recognition camera's (ANPR). Het hoofddoel van de ANPR-camera's is het constateren van overtredingen: daar is een stevige juridische basis voor in de wet met daarop gebaseerde gemeentelijke verkeersbesluiten. Maar deze camera's bieden ook de mogelijkheid analyses te maken op basis van de gescande kentekens. Dergelijke analyses kunnen laten zien hoeveel en welk type voertuigen er op welke momenten door het gebied rijden. De juridische basis voor het uitvoeren van dat soort analyses is minder duidelijk dan voor de handhaving met behulp van ANPR-camera's. Gemeenten vragen zich daarom af of het mag. In dit document wordt beschreven welke soorten analyses er mogelijk zijn en aan welke juridische voorwaarden moet worden voldaan. In hoofdstuk 1 staat meer informatie over de aanleiding voor dit onderzoek, de verzamelde informatie en de vragen waar gemeenten antwoord op willen hebben.

In hoofdstuk 2 worden drie scenario's uitgewerkt voor het soort analyses dat mogelijk is. In hoofdstuk 3 staan de koppelingen beschreven met andere bestanden om de kentekens te verrijken. In hoofdstuk 4 staan de beschermingsmaatregelen die gemeenten moeten treffen om te zorgen dat ze ook bij het maken van analyses aan de wet- en regelgeving op het gebied van privacybescherming voldoen.

Scenario 1: Analyse toegestaan

Analyse	*Juridische eisen*	*Randvoorwaarden*
• Hoeveel voertuigen rijden er? • Waar rijden de voertuigen?	• Grondslag • Doelbinding • Noodzakelijkheid • Anonieme gegevens	De kentekens moeten onomkeerbaar anoniem zijn gemaakt. Als daar twijfel over bestaat zijn extra beschermingsmaatregelen nodig en moet volgens scenario 2 worden gewerkt. ⇨ Zie hoofdstuk 2 voor meer informatie en een voorbeeld

Scenario 2: Analyse onder voorwaarden toegestaan

Analyse	*Juridische eisen*	*Randvoorwaarden*
• Welke typen voertuigen? Welke emissieklasse? • Waar komen de voertuigen vandaan? • Wat zijn de bedrijfsactiviteiten van de voertuigen? • Welke voertuigen hebben een ontheffing?	• Grondslag • Doelbinding • Noodzakelijkheid	Als openbare informatie uit het kentekenregister wordt toegevoegd is dat op zich toelaatbaar. Het gaat dan om type voertuig en emissieklasse. Maar ook dan moeten er beschermingsmaatregelen worden getroffen om te zorgen dat de niet-anonieme informatie ontoegankelijk is voor niet bevoegde functionarissen. ⇨ Zie hoofdstuk 4 voor de beschermingsmaatregelen Als de kentekens worden verrijkt met niet-openbare informatie uit externe databases, zoals adres van de kentekenhouder, bedrijfsinformatie uit het Handelsregister of het soort ontheffing, zijn extra beschermingsmaatregelen noodzakelijk. In die gevallen is het raadzaam een Data Protection Impact Assessment op te stellen. ⇨ Zie hoofdstuk 3 voor de externe databases

Scenario 3: Analyse niet toegestaan

Analyses zijn niet toegestaan als de analyse niet in lijn ligt met het doel waar de camera's voor zijn geplaatst: dan wordt immers niet voldaan aan de eis van doelbinding. Hetzelfde geldt als de analyse niet noodzakelijk is: dan is het niet rechtmatig persoonsgegevens te verwerken op de grondslag 'gerechtvaardigd belang'. Alleen als er een andere, zelfstandige grondslag in de wet is voor een ander doel (en als die analyse noodzakelijk is voor dat doel), is het alsnog mogelijk de analyse uit te voeren.

Er zijn ook analyses die op zich legitiem kunnen zijn qua doelbinding, grondslag en noodzakelijkheid, maar waarbij het niet lukt voldoende beschermingsmaatregelen te treffen die de risico's voor de privacy van betrokkenen verkleinen. Ook in dat geval is de analyse niet toegestaan.

Oplettendheid geboden

Belangrijk uitgangspunt is dat in *alle* scenario's oplettendheid vereist is. De belangrijkste juridische eis uit de Algemene Verordening Gegevensbescherming is dat informatie uitsluitend terechtkomt bij bevoegde functionarissen en dat zij zich moeten realiseren welke informatie met anderen en op welk niveau van aggregatie gedeeld mag worden. Daarom is het voor alle scenario's verstandig als de gemeentelijke projectleider die de analyses gaat uitvoeren overlegt met een privacy officer. Ook verdient het aanbeveling een werkinstructie op te stellen waarin staat op welk moment welke informatie precies door welke functionaris mag worden verwerkt. In geval van twijfel verdient het aanbeveling een Data Protection Impact Assessment op te stellen – ook voor analyses die op het eerste gezicht legitiem lijken, maar waarbij in de praktijk toch vragen opkomen over de informatiebeveiliging of privacybescherming.[1]

Noot 1 De auteurs danken Tess van den Blink voor haar voorbereidende werk in het uitzoeken van beschikbare gegevensbestanden. Ook bedanken zij Erik Regterschot en Robert Motshagen voor hun commentaar op een conceptversie van dit advies.

1 Inleiding

1.1 Aanleiding

In de meeste gemeenten met een toekomstige Zero Emissie-zone (ZE) wordt deze gehandhaafd met behulp van Automatic Number Plate Recognition camera's (ANPR). In sommige gemeenten zijn deze camera's nu al aanwezig, bijvoorbeeld omdat er al een milieuzone, een geslotenverklaring of een venstertijdengebied is ingesteld. In sommige gemeenten moeten de camera's nog worden geplaatst. De opzet van de camerasystemen is verschillend per gemeente. Het kan een volledig cordon zijn rondom het gebied waar de geslotenverklaring of milieuzone voor geldt. Maar het kunnen ook enkele, al dan niet roulerende, camera's op strategische plekken zijn.

Het hoofddoel van de ANPR-camera's is het constateren van overtredingen: daar is een stevige juridische basis voor in de wet met daarop gebaseerde gemeentelijke verkeersbesluiten. Het handhaven van de geslotenverklaringen met camera's is gebaseerd op de grondslag "gerechtvaardigd belang" en er ligt een democratisch gelegitimeerd besluit onder. Het is ook duidelijk dat er redelijkerwijs geen alternatieven zijn voor de handhaving met camera's: het is zonder camera's feitelijk onmogelijk om de handhaving uit te voeren. Er zijn ook geen lichtere middelen beschikbaar waarmee hetzelfde doel kan worden bereikt.

Maar deze camera's bieden ook de mogelijkheid analyses te maken op basis van de gescande kentekens. Dergelijke analyses kunnen laten zien hoeveel en welk type voertuigen er op welke momenten door het gebied rijden. Analyses van de verkeersstromen bieden de mogelijkheid de handhaving effectiever te maken, bijvoorbeeld door een communicatiecampagne te ontwikkelen die precies is gericht op mogelijke overtreders. De juridische basis voor het uitvoeren van dat soort analyses is echter minder duidelijk dan voor de handhaving met behulp van ANPR-camera's. Gemeenten vragen zich daarom af of het mag.

Juridische vragen: mag het?
Er is geen specifieke wet- of regelgeving die precies aangeeft onder welke voorwaarden gescande kentekens voor dit soort analyses mogen worden gebruikt. Daarom moet het advies in dit rapport worden gebaseerd op andere informatiebronnen. Dat betekent dat elk advies altijd met enige onzekerheid gepaard zal gaan. Het hangt af van het specifieke geval of het mag, rekening houdend met de omstandigheden per gemeente en met het juridische 'huiswerk' dat de gemeente heeft gedaan. Maar er zijn wel degelijk aanwijzingen dat dit soort analyses zijn toegestaan binnen de geldende wet- en regelgeving.

In het *Beoordelingskader parket CVOM voor digitale handhaving bij geslotenverklaringen en voetgangersgebieden* stond tot voor kort: "Camera's mogen enkel voor handhaving van geslotenverklaringen worden gebruikt en niet voor andere doeleinden." Dat suggereerde dat het niet was toegestaan de camera's ook voor analyses te gebruiken. Maar precies die zin is verwijderd uit de nieuwe versie van 18 april 2023. Dat is een cruciale aanpassing die meer ruimte biedt voor analyses, naast handhaving.

Ook de Autoriteit Persoonsgegevens heeft in 2021 tijdens een overleg met een gemeente bevestigd dat analyses onder bepaalde voorwaarden zijn toegestaan. Dat gebeurde in een gemeente die ANPR-camera's heeft geplaatst ter voorbereiding op een Zero Emissie-zone: de camera's werden uitsluitend geplaatst om te onderzoeken welke typen voertuigen met welke intensiteit de stad binnenkomen. Deze inzichten waren volgens de gemeente noodzakelijk om bedrijven te faciliteren en passend beleid te kunnen maken voor de daadwerkelijke invoering van de Zero Emissie-zone. De Autoriteit Persoonsgegevens liet in dat overleg weten dat in zijn algemeenheid geldt dat wanneer er een grondslag bestaat voor een bepaalde verwerking, deze grondslag ook gebruikt kan worden bij voorbereidende en direct gerelateerde verwerkingen. Met artikel 2 lid 2 sub a en artikel 14 lid 1 sub d van de Wegenverkeerswet is er een concrete grondslag voor handhaving van een milieuzone met ANPR-camera's. Omdat de ANPR-camera's in deze gemeente werden geplaatst ter voorbereiding op het instellen van een Zero Emissie-zone, kan dezelfde grondslag worden gehanteerd. Wel was het advies om vooraf duidelijk vast te leggen op welk moment een keuze wordt gemaakt voor het wel of niet instellen van een zone met handhaving. Als wordt besloten geen zone in te stellen, moet de verwerking worden

beëindigd. Deze redenering biedt dus ruimte voor analyses, mits deze direct gerelateerd zijn aan het doel waar de zone voor wordt ingesteld.

Er zijn nog meer indicaties dat analyses zijn toegestaan. Dat blijkt uit de wetgevingsgeschiedenis, de jurisprudentie en is recent bevestigd door een team van onafhankelijke experts van de Landsadvocaat (Pels Rijcken) en Verdonck, Klooster & Associates (VKA). Dit team wordt de *Adviesfunctie verantwoord datagebruik* genoemd en is opgericht door het kabinet in het kader van de Interbestuurlijke Datastrategie: een samenwerking tussen gemeenten, provincies, waterschappen en het Rijk. Doel van de strategie is de kansen van verantwoord datagebruik te benutten en knelpunten aan te pakken. Het achterliggende idee is dat initiatieven die veel maatschappelijke waarde hebben nu mislukken waardoor technologie niet goed wordt benut. Op basis van vragen uit gemeenten over meervoudig camerагebruik is in 2023 een advies opgesteld. Kort samengevat is de conclusie: “Het mag, mits...”

Met dat als uitgangspunt wordt in dit rapport een invulling aan het “mits” gegeven: een beschrijving van de randvoorwaarden waaronder gegevens uit ANPR-systemen door gemeenten mogen worden gebruikt voor analyses.

1.2 Welke analyses willen gemeenten doen?

De eerste stap in dit onderzoek was een inventarisatie van de wensen van gemeenten. Welke analyses willen zij met welke bestanden voor welke doelen doen? Eerder verzamelde informatie is gebundeld en er zijn aanvullende gesprekken gevoerd met een aantal gemeenten om hun informatiebehoefte te inventariseren. De vragen en informatie komen uit deze acht gemeenten:

Tabel 1.1 Gemeenten die informatie aanleverden

Arnhem	Leeuwarden	Utrecht
Delft	Maastricht	Zwolle
Groningen	’s-Hertogenbosch	

Gemeenten hebben behoefte aan verschillende soorten analyses. Voor een deel zijn het zeer algemene analyses, zoals over het aantal voertuigen dat het gebied in- en uitrijdt. Maar voor een deel zijn het ook zeer specifieke analyses:

- Hoeveel voertuigen rijden er het gebied in en uit?
- Zijn waarschuwingen effectief? En boetes?
- Welke typen voertuig rijden er: bestel-/vracht-/personenauto?
- Welke aandrijving/emissieklasse hebben deze voertuigen?
- Op welke dagen en uren rijden deze voertuigen het gebied in en uit?
- Uit welke gemeenten komen deze voertuigen?
- Is de eigenaar van het voertuig een particulier of een rechtspersoon?
- Welke bedrijfsactiviteiten voert de eigenaar van het voertuig uit?
- Hoeveel van de passerende voertuigen hebben een ontheffing (en welke)?

1.3 Waar maken gemeenten zich zorgen over?

De tweede stap in het onderzoek was het inventariseren van de juridische vragen waar gemeenten mee worden geconfronteerd als ze dit soort analyses willen doen. Iedereen voelt wel aan dat de ene analyse meer risico’s oplevert voor de privacy van de betrokkenen dan de andere analyse. Daarom willen gemeenten graag weten waar ze aan toe zijn en aan welke wet- en regelgeving ze precies moeten voldoen. Wat zijn de juridische kaders en welke randvoorwaarden gelden?

Het blijkt dat gemeenten zich in verschillende stadia van het zoekproces bevinden. De gemeente ‘s-Hertogenbosch wil meer inzicht krijgen in de omvang en samenstelling van logistieke stromen. Dit wordt gedaan door onder andere te koppelen met data van de RDW en Kamer van Koophandel. De gemeente hoopt dat dit

adviesrapport kan helpen bij het formuleren van een goede projectopdracht voor degenen die de analyses moeten uitvoeren.

De gemeente Utrecht doet mee aan een ander onderzoek van CBS voor statistiekdoeleinden over verkeer en logistiek. Dit onderzoek is in de afrondende fase en er is al een Data Protection Impact Assessment voor opgesteld door Privacy Company. De informatie en ervaringen uit Utrecht kunnen voor dit onderzoek ook met andere gemeenten worden gedeeld.

De gemeente Zwolle heeft het proces voor het uitvoeren van analyses om logistieke voertuigbewegingen in de binnenstad inzichtelijk te maken al helemaal ingericht. Voor de analyses worden kentekens verrijkt met open data van de RDW, maar ook met gegevens van de Kamer van Koophandel. De gegevens worden op verschillende manieren beveiligd en geanonimiseerd om de privacy van de betrokkenen te beschermen. De gemeente heeft hiervoor een Data Protection Impact Assessment opgesteld.

De gemeente Groningen heeft sinds medio 2023 een aantal camera's in de stad staan in het kader van een venstertijdengebied. De raad heeft de toezegging gekregen dat de camera's alleen worden gebruikt voor handhaving. De experts van de gemeente vragen zich daarom af of de raad moet instemmen met het gebruik van de kentekens voor het uitvoeren van analyses of dat dit binnen de definitie van handhaving past.

Alles overziend zijn dit de vragen waar een of meer gemeenten graag antwoord op willen krijgen:

- Welke gegevens van ANPR-camera's mogen worden gebruikt voor analyses?
- Mogen kentekens worden verrijkt met informatie afkomstig uit andere bestanden, bijvoorbeeld om te zien welke typen voertuigen er rijden, wie de eigenaar is en waar ze vandaan komen?
- Welke eisen worden gesteld aan de data, zoals anonimisering en bewaartermijnen?
- Moet een Data Protection Impact Assessment worden opgesteld? En een verwerkersovereenkomst?
- Moet de gemeenteraad toestemming geven voor het uitvoeren van de analyses?
- Mogen de gegevens binnen de gemeente worden gedeeld met andere afdelingen? En daarbuiten?
- Welke gemeentelijke functionarissen mogen toegang tot welke data op welk moment in het proces?

In dit rapport worden in hoofdstuk 2 drie scenario's beschreven voor de analyses die gemeenten willen doen. Sommige analyses kunnen direct op de verzamelde kentekens worden gebaseerd. Maar er zijn ook analyses waar een koppeling van kentekens met andere bestanden nodig is om de informatie te verrijken. Die andere bestanden worden besproken in hoofdstuk 3. Vervolgens gaat het in hoofdstuk 4 over de beschermingsmaatregelen die gemeenten zouden moeten treffen om te zorgen dat de analyses voldoen aan de wet- en regelgeving.

2 Drie scenario's

Globaal gesproken zijn er drie scenario's voor het maken van analyses met behulp van gescande kentekens.

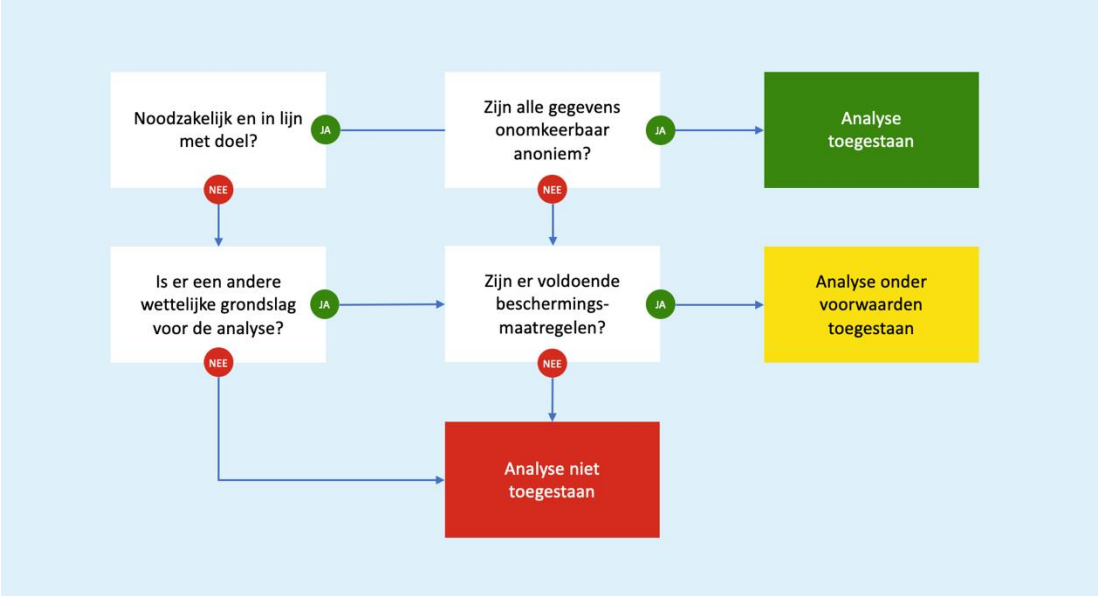
Scenario 1. Er zijn analyses die in juridische zin niet complex zijn. Analyses zijn toegestaan als ze voldoen aan vier eisen: grondslag, doelbinding, noodzaak en anonimisering. Maar ook voor dit eenvoudigste scenario gelden randvoorwaarden: er moeten niet meer gegevens worden verwerkt dan noodzakelijk en er moet goede informatiebeveiliging zijn, inclusief procedures om te controleren dat volgens de gemaakte afspraken wordt gewerkt. Vooral de eis dat kentekens anoniem moeten zijn, vraagt om voortdurende waakzaamheid omdat anonimisering in sommige gevallen toch nog kan worden teruggedraaid.

Scenario 2. Er zijn daarnaast ook analyses die een stap verder gaan qua privacy risico's. Bijvoorbeeld als het de bedoeling is de kentekens te verrijken met niet-anonieme gegevens, zoals Kamer van Koophandelnummers of bedrijfsnamen en -adressen, om te zien voor welke bedrijfsactiviteiten de voertuigen worden gebruikt en uit welke gemeenten ze vandaan komen. Ook als analyses niet voldoen aan de eis van doelbinding komt dit tweede scenario in beeld. Hieronder wordt een voorbeeld gegeven. Onder voorwaarden kunnen dit type analyses toch worden uitgevoerd, maar daar is dan wel een extra toets op rechtmatigheid voor nodig, in combinatie met extra beschermingsmaatregelen.

Scenario 3. Tot slot zijn er ook analyses denkbaar die niet zijn toegestaan. Dat is het geval als er geen grondslag is voor de analyses, als de analyses niet noodzakelijk zijn of als het niet lukt voldoende beschermingsmaatregelen te treffen om de privacy van betrokkenen te beschermen.

Schematisch ziet dat er als volgt uit: deze drie scenario's worden hieronder nader uitgewerkt.

Figuur 2.1 Drie scenario's voor analyses



2.1 Scenario 1: Analyse toegestaan

In het eerste scenario is het uitvoeren van analyses toegestaan. Om hiervoor in aanmerking te komen moet de analyse voldoen aan de volgende eisen:

- Grondslag
- Doelbinding

- Noodzakelijkheid
- Gegevens zijn onomkeerbaar anoniem gemaakt

Een voorbeeld van dit scenario komt uit een gemeente waar een milieuzone met ANPR-camera's wordt gehandhaafd. De gemeente heeft een dashboard laten ontwikkelen dat laat zien hoeveel voertuigen de milieuzone inrijden, welk percentage overtreders er is en hoe dat percentage zich ontwikkelt in de loop der tijd.

- De *grondslag* voor de plaatsing van de kentekencamera's is de Wegenverkeerswet die gemeenten het recht geeft milieuzones in te stellen. Daar moet de gemeente dan wel een Verkeersbesluit voor nemen. Als dat is geregeld, is er een grondslag voor de verwerking van de gegevens. De verwerking van de gegevens moet ook voldoen aan de AVG: ook dat is het geval. De grondslag is 'algemeen belang': artikel 6, lid 1, onder e van de AVG.
- Het maken en gebruiken van dit dashboard ligt *in lijn met het doel* van de milieuzone: het doel van de milieuzone en het doel van het dashboard zijn immers identiek.
- Daarnaast is het dashboard *noodzakelijk* om te kunnen bepalen of mensen zich houden aan de milieuzone. Het dashboard is een essentiële aanvulling om de doelstelling van de milieuzone te kunnen bereiken.
- In het dashboard worden geen afzonderlijke kentekens getoond: het is immers niet nodig om te weten *welke* voertuigen de milieuzone in zijn gereden. De informatie in het dashboard wordt getoond is onomkeerbaar anoniem gemaakt. Een gebruiker van het dashboard kan onmogelijk achterhalen welke voertuigen de milieuzone in zijn gereden.

Elke gemeente kan op deze manier zelf beredeneren of een bepaalde analyse is toegestaan: een controle of aan de vier voorwaarden wordt voldaan is voldoende. In dat geval is het risico voor de fundamentele rechten en vrijheden van de betrokkenen tot een acceptabel niveau verlaagd. Voor deze verwerking moeten wel beschermingsmaatregelen worden getroffen. De informatie over de kentekens die in het dashboard wordt gebruikt moet namelijk wel echt onomkeerbaar anoniem zijn. Dat is makkelijker gezegd dan gedaan – zie het kader 'Over anonimisering' hieronder en zie de beschermingsmaatregelen aan het eind van dit rapport.

2.2 Scenario 2: Analyse onder voorwaarden toegestaan

In het tweede scenario zijn analyses ook toegestaan, maar onder voorwaarden. Er zijn twee 'routes' die tot dit scenario leiden.

Het eerste voorbeeld is een analyse waarbij het niet lukt de kentekens die voor de analyse nodig zijn aantoonbaar en onomkeerbaar anoniem te maken. Of als het nodig is de kentekens te verrijken met informatie uit andere bestanden waardoor de kentekens kunnen worden herleid tot een individu. Een bedrijfsnaam of adres valt ook in die categorie: het is weliswaar geen directe link naar een natuurlijk persoon, maar wel een indirecte link. In dat geval zullen extra beschermingsmaatregelen moeten worden getroffen om te zorgen dat de privacy van de betrokkenen voldoende wordt gerespecteerd. Als dat lukt, is het alsnog toegestaan de analyses uit te voeren. Maar dan moeten de privacy risico's voor de betrokkenen wel voldoende worden beperkt. Dat vergt het maken van een risico-inschatting en een afweging van de risico's enerzijds en het belang van de gemeente bij het uitvoeren van de analyses anderzijds. Later in dit advies wordt een overzicht gegeven van mogelijke beschermingsmaatregelen, zowel technisch als organisatorisch. De beste manier om aantoonbaar aan de wet te voldoen is door het opstellen van een Data Protection Impact Assessment. Dat moet de uitvoerder van de analyses niet in zijn eentje doen, maar in samenwerking met een privacyfunctionaris van de gemeente, een informatiebeveiliger en technische experts. Meer hierover aan het eind van het rapport.

Het tweede voorbeeld waar dit scenario zich voordoet, is als er behoefte is aan analyses die niet in lijn liggen met het oorspronkelijke doel waar de ANPR-camera's voor zijn geplaatst. Een voorbeeld is het maken van een analyse voor de afdeling Economische Zaken die een communicatiecampagne wil ontwikkelen om de aantrekkelijkheid van de binnenstad voor bedrijven te vergroten. Dat doel ligt niet in lijn met het doel waar de ANPR-camera's voor zijn geplaatst: handhaving van de geslotenverklaring. Daarom is deze analyse niet zonder meer toegestaan. Maar onder voorwaarden is het wel degelijk mogelijk. Hiervoor gelden dan dezelfde eisen als in scenario 1: grondslagvereiste, doelbindingsvereiste en de noodzakelijkheidseis. Dat betekent dat moet worden uitgezocht of er een wettelijke taak of bevoegdheid is voor het uitvoeren van de gewenste andere

analyses (grondslag) en of die analyse in lijn ligt van die taak of bevoegdheid (doelbinding). Als de analyse vervolgens ook aantoonbaar noodzakelijk is voor het bereiken van het doel én als er voldoende beschermingsmaatregelen worden getroffen, is de analyse alsnog toegestaan.

Over anonimisering

De Europese toezichthouders, dus ook de Nederlandse Autoriteit Persoonsgegevens, werken samen in de European Data Protection Board. Deze samenwerking is de opvolger van de Artikel 29 Werkgroep. De EDPB neemt het standpunt in dat alleen sprake is van anonieme gegevens als iedere mogelijkheid tot identificatie van de betrokkene onherroepelijk is uitgesloten. Dat betekent dat herleidbaarheid, koppelbaarheid en deduceerbaarheid (redelijkerwijs) onmogelijk moeten zijn. Elke mogelijkheid tot identificatie moet onomkeerbaar worden uitgesloten. In 2014 bleek uit een analyse van anonimiseringstechnieken dat volledige anonimiteit in veel gevallen moeilijk te bereiken is: geen van de onderzochte technieken voldeed met zekerheid aan de gestelde eisen. Ook als een 'slimme' camera geen mensen of kentekens 'ziet' kunnen er technische mogelijkheden zijn om toegang te krijgen tot die gegevens, bijvoorbeeld door software-instellingen te wijzigen. Maar er zijn ook technieken die privacy risico's geheel of ten dele kunnen ondervangen, vooral door combinatie van verschillende technieken. In het hoofdstuk over beschermingsmaatregelen staan voorbeelden van mitigerende maatregelen.

De parlementaire geschiedenis en de rechtspraak bieden ruimte voor een minder strakke interpretatie van anonimisering, maar in de adviezen en boetebesluiten van de Autoriteit Persoonsgegevens wordt de striktere lijn gehanteerd. Het is daarom van groot belang dat de analyses op *aantoonbaar* anoniem gemaakte gegevens worden gebaseerd. Het is niet genoeg om te verwijzen naar een verzoek aan een leverancier om gegevens te anonimiseren: het proces moet zo concreet mogelijk worden uitgewerkt en schriftelijk vastgelegd.

Het anonimiseren van kentekens is zelf wel een verwerking van persoonsgegevens, dus de partij die de gegevens anonimiseert en aanlevert voor de analyses moet voor dat deel van het analyseproces wel degelijk aan de Algemene Verordening Gegevensbescherming voldoen. En als een koppeling wordt gelegd met andere bestanden, zoals adresgegevens of de naam van de kentekenhouder, worden alsnog persoonsgegevens verwerkt. In dat geval zijn de gegevens dus niet anoniem en moeten extra beschermingsmaatregelen worden getroffen.

Bij twijfel over de onomkeerbaarheid van de anonimisering, verdient het aanbeveling om de gegevens te beschouwen als persoonsgegevens en aanvullende beschermingsmaatregelen te treffen. Aangezien al eerder is vastgesteld dat de analyses voldoen aan het grondslagvereiste (er is een juridische basis voor), doelbindingsvereiste (de analyse ligt in lijn met het doel van de oorspronkelijke verwerking) en aan de noodzakelijkheidseis (de analyse is noodzakelijk voor het bereiken van het doel) is het ook toegestaan niet-anonieme persoonsgegevens te verwerken. Maar daar moeten wel

2.3 Scenario 3: Analyse niet toegestaan

Analyses zijn niet toegestaan als de analyse niet in lijn ligt met het doel waar de camera's voor zijn geplaatst: dan wordt immers niet voldaan aan de eis van doelbinding. Hetzelfde geldt als de analyse niet noodzakelijk is: dan is het niet rechtmatig persoonsgegevens te verwerken. Alleen als er een andere, zelfstandige grondslag in de wet is gecreëerd voor het andere doel (en als de analyse noodzakelijk is om dat doel te bereiken), is het alsnog mogelijk de analyse uit te voeren. Dan moet de grondslag voor de verwerking dus wel worden aangepast.

Er zijn ook analyses die op zich legitiem zijn qua doelbinding, grondslag en noodzakelijkheid, maar waarbij het niet lukt voldoende beschermingsmaatregelen te treffen die de risico's voor de privacy van betrokkenen verkleinen. Ook in dat geval is de analyse niet toegestaan.

3 Koppeling met andere bestanden

Om een overzicht te maken van het aantal voertuigen per dag, tijd en plek is het niet nodig om te weten om welke kentekens het ging. Die analyses kunnen dus worden uitgevoerd met geanonimiseerde en geaggregeerde gegevens. Dan is geen sprake van verwerking van persoonsgegevens en valt de verwerking in scenario 1 hierboven.

Maar sommige gemeenten willen analyses uitvoeren die verder gaan dan anonieme informatie. Zij willen de gescande kentekens verrijken met informatie uit andere bestanden. In dat geval is altijd sprake van scenario 2 (toegestaan onder voorwaarden) of scenario 3 (niet toegestaan).

Op basis van de behoeften van gemeenten komen drie soorten externe bestanden in aanmerking: de kentekenregistratie van de RDW, het Handelsregister en databases met ontheffingen. Die worden hieronder beschreven.

Tabel 3.1 Soorten analyses en externe data

Soort analyse	Externe data
Hoeveel voertuigen rijden er?	(geen)
Waar rijden de voertuigen?	(geen)
Welke typen voertuigen? Welke emissieklasse?	Online Voertuig Informatie RDW
Waar komen de voertuigen vandaan?	Kentekenregister RDW
Wat zijn de bedrijfsactiviteiten van de voertuigen?	Stap 1: Kentekenregister RDW Stap 2: Handelsregister
Hoeveel voertuigen hebben een ontheffing?	Ontheffingendatabase

In het algemeen kan hier reeds worden geconstateerd dat koppeling met externe data in alle gevallen leidt tot scenario 2 (toegestaan onder voorwaarden) of scenario 3 (niet toegestaan). Want de kentekens kunnen niet worden geanonimiseerd als ze moeten worden gekoppeld met andere data. Dat vergroot de kans dat ergens in het proces van de analyses kentekens of andere persoonsgegevens zichtbaar zijn en daarmee gaan dit soort analyses dus een stap verder dan analyses op anonieme data. Dat wil niet zeggen dat het niet is toegestaan: het betekent wel dat de risico's zorgvuldig moeten worden geïnventariseerd en gemitigeerd.

3.1 Online Voertuig Informatie RDW

Het kentekenregister bevat informatie over voertuigen en wordt beheerd door de Dienst Wegverkeer (RDW). In het Besluit Aanwijzing toezichthouders gebruik gegevens kentekenregister staat welke informatie over kentekens kan worden opgevraagd en gebruikt. De informatie is onderverdeeld in gevoelige en niet-gevoelige gegeven. De niet-gevoelige gegevens mogen aan eenieder worden verstrekt. Als de analyses van een gemeente beperkt blijven tot de niet-gevoelige gegevens is de inbreuk op de privacy van de kentekenhouders dus beperkt.

Als ook gevoelige gegevens worden gekoppeld is het risico voor de privacy van betrokkenen veel groter. Gevoelige gegeven zijn persoonsgegevens, concurrentiegevoelige gegevens en fraudegevoelige gegevens. Voor die gevoelige gegevens geldt een restrictief verstrekkingenbeleid, uitgewerkt in het Kentekenreglement, een aantal ministeriële regelingen en een reglement van de Dienst Wegverkeer. Het is evident dat analyses van kentekens die zijn verrijkt met gevoelige gegevens grotere risico's opleveren voor de privacy van de betrokkenen dan analyses die zijn gebaseerd op de niet-gevoelige gegevens.

Openbare informatie, niet-gevoelige gegevens
Veel informatie over voertuigen is openbaar beschikbaar op de website van de RDW. Voor veel van de analyses waar gemeenten behoefte aan hebben is het voldoende om van deze niet-gevoelige gegevens gebruik te

maken. Dat levert qua privacybescherming geen grote risico's op en dus kan het aantal beschermingsmaatregelen beperkt blijven. Het gaat om de volgende informatie:

Basis
Algemeen (Voertuigcategorie, Carrosserietype, Inrichting, Merk, Kleur, Aantal eigenaren privé / zakelijk)
Vervaldata en historie (APK, datum eerste tenaamstelling in NL, datum laatste tenaamstelling e.d.)
Gewichten (Massa rijklaar / ledig voertuig, Technische max. massa e.d.)
Tellerstanden (Jaar laatste registratie, Oordeel, Toelichting)
Status van het voertuig (Gestolen, Geëxporteerd, WAM verzekerd e.d.)
Terugroepacties

Motor & Milieu
Brandstof, Geluidsniveau, Emissieklasse, Nettomaximumvermogen, e.d.

Technisch
Aantal zitplaatsen, Aantal assen / wielen, Wielbasis e.d.

Fiscaal
Bruto BPM, Catalogusprijs

Als het lukt om de kentekens direct na het scannen te laten verrijken met dit soort informatie en de kentekens daarna onomkeerbaar te anonimiseren voordat ze worden geanalyseerd, levert dat een verwerking met een laag risico op. Als de verrijking later in het proces plaatsvindt en de data dus door meer functionarissen kunnen worden ingezien, levert dat een verwerking met een hoog risico op waar meer beschermingsmaatregelen nodig zijn.

3.2 Kentekenregister RDW: postcodecijfers

Sommige gemeenten willen een stap verder gaan met het kentekenregister dan de openbare informatie. Zij willen bijvoorbeeld weten waar de voertuigen vandaan komen die in het gebied rijden. Dat kan nodig zijn om een effectieve communicatiecampagne te kunnen ontwerpen. Als vooral voertuigen van buiten de gemeente zich niet aan de regels houden, heeft het immers weinig zin om inwoners en ondernemers binnen de gemeente informatie aan te bieden. Het heeft dan meer zin een landelijke campagne te starten – in samenwerking met andere gemeenten die met geslotenverklaringen werken. Of een gerichte campagne voor bedrijven in bepaalde gemeenten. Daar zijn adresgegevens voor nodig van de voertuigen die door de ANPR-camera's zijn gescand en dat gaat een stuk verder dan de openbare gegevens over kentekenhouders.

Niet openbare informatie, gevoelige gegevens
Om te kunnen achterhalen waar een voertuig vandaan komt moet het kenteken worden gekoppeld aan de postcode. In de Regeling gegevensverstrekking kentekenregister 2008 staat onder welke voorwaarden dat mogelijk is. Het advies is om voor het achterhalen van de herkomst van een voertuig alleen het numerieke deel van de postcode te gebruiken: dus de vier cijfers. Als ook de twee letters worden toegevoegd, wordt de informatie gevoeliger – zonder dat de analyses er inhoudelijk beter bruikbaar door worden. Maar zelfs als het kenteken wordt gecombineerd met alleen het numerieke deel van de postcode, wordt die combinatie al beschouwd als gevoelige gegevens. Deze gegevens mogen worden verstrekt voor statistische doeleinden, maar alleen aan informatieproviders of voor wetenschappelijke doeleinden. Dat geldt dus niet voor overheden. Maar in artikel 42 van de Wegenverkeerswet is een interessante uitzondering opgenomen die ruimte biedt voor het verstrekken van gegevens uit het kentekenregister voor analyses. In artikel 42, lid 4, onder c staat dat de Dienst Wegverkeer in het kentekenregister gegevens over motorrijtuigen en aanhangwagens verwerkt met als een van de doelen: "Om overheidsorganen te voorzien van gegevens uit het kentekenregister voor zover zij aangeven deze gegevens nodig te hebben voor een goede uitoefening van hun publieke taak".

Er wordt in deze wet geen onderscheid gemaakt tussen gevoelige en niet-gevoelige gegevens. Dat betekent dat de postcode-gegevens uit het kentekenregister onder voorwaarden ook mogen worden gebruikt door gemeenten voor het uitvoeren van bepaalde analyses. Maar daarbij geldt dus wel de eis dat de gemeente deze gegevens nodig moet hebben voor een goede uitoefening van hun publieke taak. Dat betekent ten eerste dat de gemeente het besluit moet hebben genomen een gebied af te sluiten voor (bepaalde) voertuigen op basis van die publieke taak. Dat is de grondslag waarop de ANPR-camera's zijn geplaatst. Maar dat is niet genoeg als

onderbouwing voor het koppelen van kentekens met persoonsgegevens. Daarom moet, ten tweede, een besluit worden genomen door de gemeente waarin staat dat koppeling van de gescande kentekens aan de postcode (of het Kamer van Koophandelnummer) nodig is voor het goed uitoefenen van de publieke taak.

3.3 Kamer van Koophandel: Standaard Bedrijfs Indeling

Voor sommige gemeenten is het belangrijk te weten waarom voertuigen in het afgesloten gebied rijden. Ze willen weten of de voertuigen van een bedrijf (of een andere rechtspersoon) of een particulier (natuurlijk persoon) zijn. En als het een bedrijf is, willen ze weten welke activiteiten dat bedrijf uitvoert. Daarvoor is een koppeling in twee stappen nodig. Eerst moet het kenteken worden opgezocht in het kentekenregister om het Kamer van Koophandelnummer te achterhalen. Van rechtspersonen en erkende bedrijven is het Kamer van Koophandelnummer geregistreerd in het kentekenregister.

De tweede stap is het opzoeken van extra informatie in het Handelsregister op basis van het Kamer van Koophandelnummer. In het Handelsregister staan basisgegevens over rechtspersonen, zoals de maatschappelijke activiteit, gegevens van de eigenaar, gegevens van de hoofdvestiging en een link naar de vestigingenlijst. Voor de analyses waar het in dit rapport over gaat, is eigenlijk alleen de maatschappelijke activiteit interessant. Want de overige adresgegevens zijn direct op te vragen in het kentekenregister – daar is geen koppeling met het Handelsregister voor nodig.

Als het Kamer van Koophandelnummer bekend is, kan worden uitgezocht welke activiteiten een onderneming heeft. De Kamer van Koophandel biedt externen de mogelijkheid basisgegevens op te vragen via een directe koppeling met hun database (via een API). Daaraan zijn kosten verbonden: € 0,018 per bevraging. De service is 24 uur per dag beschikbaar, maar per maand mogen maximaal 300.000 bevragingen worden gedaan en de snelheidslimiet is 100 bevragingen per seconde.

Elk bedrijf staat in het Handelsregister met een code van 4 of 5 cijfers volgens de Standaard Bedrijfs Indeling. Deze informatie kan op verschillende aggregatieniveaus worden geanalyseerd. Het hoogste – meest anonieme – niveau zijn de algemene categorieën, zoals Landbouw, Industrie en Bouwnijverheid. In dat geval is de kans vrijwel nihil dat op basis van de code kan worden achterhaald om welke onderneming het ging. Analyses op dat niveau leveren dus beperkte risico's voor de privacy van betrokkenen op.

Maar het is ook mogelijk veel specifiekere informatie te vinden. Onder de algemene categorie *Detailhandel* (47) vallen bijvoorbeeld *Winkels in consumentenelektronica* (47.4) met daaronder nog een verdere opsplitsing in bijvoorbeeld *Winkels in audio- en videoapparatuur* (47.43.1). Ander voorbeeld: onder de algemene categorie *Logies-, maaltijd- en drankverstrekking* (I) kan worden ingezoomd tot op de specifieke activiteit *Eventcatering* (56.21).

Naarmate de informatie specifieker wordt, wordt de kans groter dat er een unieke link kan worden gelegd met een specifieke onderneming. Als de analyses worden uitgevoerd op zo'n hoog aggregatieniveau dat het over vele duizenden ondernemingen kan gaan, is het risico op identificatie van een individu verwaarloosbaar. Daar moet dus een optimum worden gevonden tussen het gewenste detailniveau van de informatie en het beschermen van de privacy van betrokkenen.

Vervolgens moeten beschermingsmaatregelen worden getroffen die passen bij de gevoeligheid van de gegevens. De mogelijke beschermingsmaatregelen worden later in dit rapport besproken.

Als de onderneming een eenmanszaak is, levert dat direct een link met een specifiek individu op. Dit is echter geen probleem dat zich in de praktijk kan voordoen, aangezien een eenmanszaak geen rechtspersoon is, maar een natuurlijke persoon. Daar kunnen in het Handelsregister geen inschrijvingen van worden opgevraagd.

3.4 Ontheffingendatabase

Mensen die toestemming willen krijgen om van bepaalde verkeersregels af te wijken moeten een ontheffing voor hun voertuig aanvragen. Dit wordt een RVV-ontheffing of -vrijstelling genoemd (RVV = Reglement verkeersregels en verkeerstekens).

Welke databases zijn interessant?
De ontheffingen staan in verschillende databases geregistreerd. Er zijn landelijke ontheffingen, bijvoorbeeld voor bedrijven die in heel Nederland graafwerkzaamheden moeten verrichten en om die reden hun voertuigen moeten neerzetten op plekken waar dat zonder ontheffing niet is toegestaan. Er zijn ook ontheffingen voor provinciale wegen en waterschappen, bijvoorbeeld voor het rijden op een busbaan. De interessantste databestanden voor de analyses waar het in dit rapport over gaat, zijn de gemeentelijke ontheffingen. Want die ontheffingen laten zien waarom een voertuig in het afgesloten gebied rijdt. Het kan bijvoorbeeld gaan om verhuizers, stratenmakers, deurwaarders of medewerkers in de zorg. Voor dat soort doelen kan in de meeste gemeenten een verkeersontheffing voor de hele gemeente worden aangevraagd. Voor toegang tot een afgesloten gebied is daarnaast vaak een aparte ontheffing nodig die ook wordt geregistreerd door de gemeente. In die lokale database met ontheffingen voor de geslotenverklaring(en) staan de kentekens van voertuigen die een dagontheffing hebben aangevraagd. Maar ook ontheffingen om andere redenen worden daarin geregistreerd, zoals ontheffing om medische redenen, financiële noodzaak of bijzondere situaties.

De gemeenten die een Zero Emissie-zone willen instellen hebben het plan opgevat een Centraal Loket op te tuigen voor een centraal register voor de handhaving. Twintig gemeenten hebben daarvoor een Intentieovereenkomst ondertekend. Het is de bedoeling dat de RDW dit Centraal Loket gaat beheren. Voor de juridische consequenties is die ontwikkeling overigens niet zo relevant. Of analyses nu op een lokale database met ontheffingen worden gebaseerd of op het Centraal Loket maakt voor de juridische haalbaarheid niet veel uit.

Anonieme en geaggregeerde analyses zijn toegestaan, met beperkte beschermingsmaatregelen
Het antwoord op de vraag of het is toegestaan analyses uit te voeren die kijken naar ontheffingen, hangt af van de vraag hoe gedetailleerd de informatie is die wordt gerapporteerd. Sowieso is bij deze koppeling sprake van scenario 2 of scenario 3 omdat de gegevens niet anoniem zijn: het kenteken is nodig om te zien of het een ontheffing heeft. Uitgaand van een analyse die in lijn ligt met het doel waar de kentekens voor zijn verzameld (bijvoorbeeld handhaving van een milieuzone of Zero Emissie-zone) en uitgaand van de aanname dat de analyse noodzakelijk is, is het mogelijk te onderbouwen waarom analyses binnen de wet- en regelgeving zijn toegestaan. Een voorbeeld van zo'n analyse is een rapportage waarin staat welk percentage van de gescande voertuigen een ontheffing heeft. In de simpelste analyse wordt geen opsplitsing gemaakt naar de reden voor de ontheffing. Het is dan dus niet bekend of het voertuig een dagontheffing had of een ontheffing voor lange tijd. Dat soort informatie willen gemeenten vaak wel hebben. Verdere opsplitsing is mogelijk maar alleen onder de voorwaarde dat het onmogelijk moet zijn om van de gerapporteerde percentages terug te gaan naar een specifiek kenteken. In dat geval zijn dit soort analyses mogelijk met een beperkt aantal beschermingsmaatregelen.

Medische informatie mag in principe niet worden verwerkt
Als in een analyse ook medische gegevens over personen worden verwerkt, is het risico voor de privacy van de betrokkenen veel groter. Gegevens over gezondheid vallen volgens de Algemene Verordening Gegevensbescherming (artikel 9, lid 1 AVG) onder de bijzondere categorieën van persoonsgegevens. Dit worden ook wel "gevoelige gegevens" genoemd. Verwerking van dat soort gegevens is in principe verboden. De AVG biedt wel ruimte voor verwerking van gezondheidsgegevens als dat noodzakelijk is voor gezondheidsdoeleinden, zoals de volksgezondheid en de preventie of bestrijding van ernstige gezondheidsbedreigingen. Maar er zijn meer uitzonderingen. De meest voor de hand liggende uitzondering in dit kader is dat de verwerking in het belang moet zijn van natuurlijke personen en de samenleving als geheel. Daarom mag een gemeente een database met ontheffingen aanleggen, ook al moet daar medische informatie voor worden verwerkt. Het is onvermijdelijk deze informatie te verwerken: het doel kan immers niet worden bereikt zonder die medische informatie.
Maar voor het uitvoeren van de analyses waar dit advies over gaat is het niet nodig medische informatie te verwerken. De analyse kan immers ook zonder die informatie worden uitgevoerd. Dus mag geen medische informatie worden verwerkt. Dat zou alleen mogen als de wetgever zou besluiten een specifieke wettelijke grondslag met passende waarborgen ter bescherming van de persoonsgegevens en andere grondrechten te maken. Dat ligt niet in de lijn der verwachting – ook omdat dit soort gegevens dan zonder toestemming van de betrokkene zullen worden verwerkt. De AVG stelt hoge eisen aan verwerkers van dat soort gegevens om

passende en specifieke maatregelen te treffen ter bescherming van de rechten en vrijheden. Het is dus aannemelijk dat analyses die ook gebaseerd zijn op gegevens over gezondheid niet zijn toegestaan.

De conclusie is dus dat het koppelen aan een ontheffingsdatabase wel kan worden onderbouwd voor geaggregeerde gegevens (wel/geen ontheffing). Dat is met een beperkt aantal beschermingsmaatregelen mogelijk. Het is niet mogelijk analyses uit te voeren als daar medische informatie over individuen voor nodig is. Geaggregeerde analyses op onomkeerbaar geanonimiseerde persoonsgegevens zijn wel toegestaan – mits de anonimisering echt onomkeerbaar is.

3.5 Samenvattend

Hier worden de soorten analyses die gemeenten zouden willen doen, achtereenvolgens besproken. De gekozen volgorde loopt van verwerkingen met een relatief laag risico naar relatief hoog risico.

Hoeveel voertuigen rijden er? Waar rijden de voertuigen?
Deze analyses vergen geen koppeling aan andere databases en de kentekens kunnen anoniem worden verwerkt. Als de gegevens aantoonbaar onomkeerbaar anoniem zijn, en als de analyse in lijn ligt met de doelstelling waar de ANPR-camera's voor zijn geplaatst, is scenario 1 van toepassing. Anonieme tellingen bevatten geen persoonsgegevens en kunnen dus worden verwerkt. Het verdient wel aanbeveling de juridische onderbouwing schriftelijk vast te leggen, waarin ook duidelijk wordt gemaakt dat de anonieme gegevens onmogelijk kunnen worden herleid naar het oorspronkelijke kenteken. Ook verdient het aanbeveling analyses te doen op grote aantallen voertuigen en dus niet per camera per minuut. Dat verkleint de kans dat de informatie tot een specifieke persoon te herleiden is.

Welke typen voertuigen? Welke emissieklasse?
Deze analyses vereisen koppeling met openbare informatie uit de Online Voertuig Informatie van de RDW. Dat is onder voorwaarden toegestaan. De belangrijkste voorwaarden zijn dat de analyses in lijn moeten liggen met het doel waar de camera's voor zijn neergezet. Als de camera's zijn neergezet voor een milieuzone of Zero Emissie-zone is het logisch dat koppeling van het kenteken met het voertuigtype of de emissieklasse van het voertuig nodig is. Voor andere doelen geldt die redenering niet. Overigens moet voor deze analyses ook een zorgvuldige afweging worden gemaakt van de risico's en moeten afdoende beschermingsmaatregelen worden getroffen om te zorgen dat aantoonbaar aan de wet- en regelgeving wordt voldaan. Zo vroeg mogelijk in het proces (en onomkeerbaar) anonimiseren van de kentekens is een belangrijke maatregel. Het doet er voor de analyses immers niet toe *welk* kenteken is gescand: het gaat alleen om de aantallen per voertuigtype of emissieklasse.

Waar komen de voertuigen vandaan?
Analyses die laten zien waar voertuigen vandaan komen zijn alleen mogelijk op data die worden verrijkt met niet-anonieme en niet-openbare informatie uit het kentekenregister. Dat betekent dat de risico's voor de privacy van de betrokkenen veel groter zijn dan bij de analyses die hierboven werden beschreven. Toch kan het onder voorwaarden mogelijk zijn dit soort analyses te doen. Uiteraard moet worden voldaan aan de voorwaarden die altijd gelden: grondslag, doelbinding en noodzaak. Daarnaast is het belangrijk – net als bij de analyses van voertuigtypen en emissieklassen – dat data zo vroeg mogelijk in het proces (en onomkeerbaar) anoniem te maken. Omdat er verschillende databestanden worden gekoppeld en omdat één van die databestanden niet openbaar is, vereist dit een grondige uitwerking in de vorm van een Data Protection Impact Assessment. Daarin moet worden beschreven hoe de kentekengegevens precies worden verwerkt en op welk moment en op welke manier ze worden geanonimiseerd. Om te zorgen dat de risico's voldoende worden beperkt, moeten stevige beschermingsmaatregelen worden getroffen. Voorbeelden staan in het volgende hoofdstuk.

Wat zijn de bedrijfsactiviteiten van de voertuigen?
Voor deze analyses moeten de kentekens worden verrijkt met informatie uit twee andere bestanden: het kentekenregister van de RDW (niet-openbare informatie) en het Handelsregister. Dat levert uiteraard nog meer risico's op dan de bovenstaande analyses: hoe meer koppelingen, hoe groter de kans dat gevoelige informatie bij een onbevoegde persoon terechtkomt. Daarom is het verstandig voor deze analyses – naast de algemene eisen van grondslag, doelbinding en noodzaak – te voldoen aan minstens hetzelfde niveau van risicomitigatie als

voor de analyses waar de herkomst van de voertuigen wordt gebruikt. In een Data Protection Impact Assessment moet precies worden beschreven welke risico's zich kunnen voordoen in het proces en welke maatregelen worden getroffen om die te mitigeren. Een goed idee is om de informatie 'zo anoniem mogelijk' te analyseren. Voor de meeste analyses is het waarschijnlijk voldoende om de bedrijfsinformatie te aggregeren op een niveau waarop identificatie van een afzonderlijk bedrijf (of de eigenaar in het geval van een eenmanszaak) onmogelijk is. Dus niet 'Eventcatering', maar de bredere categorie 'Logies-, maaltijd- en drankverstrekking'. En niet: 'Winkel in consumentenelektronica', maar de bredere categorie 'Detailhandel'.

Hoeveel voertuigen hebben een ontheffing?

Dit is van de mogelijke analyses de meest riskante. Want ontheffingen worden voor een deel verleend om medische redenen en gezondheidsinformatie valt volgens de AVG in de categorie bijzondere persoonsgegevens. Bijzondere persoonsgegevens mogen in principe niet worden verwerkt, tenzij aan een van de voorwaarden van artikel 9 lid 2, AVG is voldaan. Daarvan is hier geen sprake. Informatie over ontheffingen kan dus niet op het gedetailleerde niveau van gezondheidsinformatie worden verwerkt. Als de medische informatie onmogelijk kan worden gekoppeld aan een individueel kenteken (door anonimisering) is een analyse wel toegestaan. Maar dan moeten de kentekens wel onomkeerbaar anoniem zijn gemaakt. Een alternatief dat nog makkelijker is en wellicht voldoende informatie oplevert voor de gemeente is een analyse die onderscheid maakt tussen tijdelijke en langdurige ontheffingen. Dan wordt geen gezondheidsinformatie verwerkt. Ook daar is het echter nodig om (naast de algemene eisen van grondslag, doelbinding en noodzaak) te voldoen aan de strikte eisen op het gebied van informatiebeveiliging en privacybescherming. En ook hier is het dus raadzaam een Data Protection Impact Assessment op te stellen. Daarin moeten waarborgen worden getroffen in de vorm van technische en organisatorische maatregelen, inclusief controles en toezicht. Het volgende hoofdstuk beschrijft hoe dat werkt.

4 Beschermingsmaatregelen

In het tweede hoofdstuk zijn drie scenario's beschreven waar analyses in kunnen vallen. In het derde hoofdstuk ging het over het koppelen van kentekens aan andere bestanden om de informatie te verrijken. In dit hoofdstuk worden de randvoorwaarden beschreven waar dat soort analyses aan moeten voldoen. Het uitvoeren van analyses op gescande kentekens levert namelijk altijd een risico op voor de privacy van de betrokkenen. Dat betekent dat in alle gevallen randvoorwaarden gelden om te zorgen dat analyses aantoonbaar aan de AVG voldoen.

4.1 Basisvoorwaarden: grondslag, doelbinding en noodzaak

Scenario 1: Toegestaan, maar met onomkeerbaar geanonimiseerde gegevens
De meest basale analyse geeft antwoord op de vraag: "Hoeveel voertuigen rijden er?" of "Waar rijden voertuigen?" Voor alle analyses – dus ook voor analyses volgens dit scenario 1 – geldt dat er een grondslag voor moet zijn, dat sprake moet zijn van doelbinding en dat de analyses noodzakelijk moeten zijn. Als het goed is zijn deze zaken allemaal al uitgewerkt in de Data Protection Impact Assessment die is opgesteld voorafgaand aan het plaatsen van de ANPR-camera's. In die gevallen zijn analyses op geanonimiseerde gegevens toegestaan, als ze gebaseerd worden op dezelfde grondslag, doelbinding en noodzaak. Om volgens dit scenario 1 te kunnen werken, mogen de kentekens niet worden gekoppeld aan andere bestanden. En ze moeten onomkeerbaar anoniem zijn gemaakt. Zoals gezegd hanteert de Autoriteit Persoonsgegevens een strakke definitie van anonimisering. Want geanonimiseerde gegevens kunnen in sommige gevallen toch nog worden herleid naar een individueel kenteken en dus naar een individu. Als twijfels bestaan (of kunnen ontstaan) over de anonimisering kan het raadzaam zijn voor de zekerheid ook voor dit type analyses de beschermingsmaatregelen te treffen die gelden voor scenario 2.

Scenario 2: Aanvullende Data Protection Impact Assessment voor de analyses
Een stap verder gaan de analyses die onderscheid maken naar type voertuig, emissieklasse, herkomst, bedrijfsactiviteiten en (type) ontheffing. Bij de analyses in dit scenario 2 verdient het aanbeveling een Data Protection Impact Assessment op te stellen – specifiek voor de analyses die uitgevoerd zullen worden. Dat is een document dat beschrijft hoe het proces van gegevensverwerking zal verlopen. Daarnaast wordt beschreven waarom het rechtmatig (grondslag en doelbinding) en noodzakelijk is de gegevens te verwerken. Tot slot worden de privacy risico's geïnventariseerd en worden beschermingsmaatregelen beschreven om de risico's weg te nemen of te verkleinen.
Voor het opstellen van een DPIA is een projectteam nodig waarin alle deskundigheid aan tafel zit. De proceseigenaar (dat is de gemeentelijke afdeling die de analyses wil uitvoeren), aangevuld met een privacy officer, een informatiebeveiliger en eventueel de afdeling onderzoek of een externe organisatie die de analyses daadwerkelijk zal gaan uitvoeren. Dit team moet bij elkaar komen om input voor de DPIA te leveren. Daarna moet de DPIA voor advies aan de gemeentelijke Functionaris voor Gegevensbescherming worden voorgelegd. Op basis van dat advies kan de DPIA worden aangepast. Daarna kan de verwerkingsverantwoordelijke de DPIA vaststellen en kan de verwerking beginnen.

Scenario 3: Niet toegestaan
Het is ook denkbaar dat gemeenten analyses willen doen die niet in lijn liggen met het doel waar de camera's voor zijn geplaatst. Een (extreem) voorbeeld is het verkopen van de database met gescande kentekens aan een bedrijf voor direct marketing. Dat is niet toegestaan. Ook als niet wordt voldaan aan de eisen van een grondslag, doelbinding en noodzakelijkheid zijn analyses niet toegestaan. Een voorbeeld van een analyse die niet noodzakelijk is, is een onderzoek naar geluidsoverlast door voertuigen. Het is voor het meten van geluid niet noodzakelijk kentekens te scannen: een microfoon die decibels meet is een prima alternatief omdat er geen persoonsgegevens worden verwerkt. Zelfs als een analyse wel aan alle eisen voldoet (dus grondslag, doelbinding en noodzakelijk) is het mogelijk dat de analyse toch niet is toegestaan. Dat is het geval als het niet lukt om de risico's voldoende te verkleinen. In dat geval kan een analyse die in eerste instantie als een scenario 2 werd beschouwd, alsnog onmogelijk blijken te zijn.

4.2 Beschermingsmaatregelen: technisch

Hier worden voorbeelden gegeven van beschermingsmaatregelen die risico's kunnen wegnemen of verkleinen. Daarbij maken we onderscheid tussen technische maatregelen en organisatorische maatregelen. De combinatie van beide soorten maatregelen is vaak nodig om de bruto risico's van een verwerking tot een acceptabel netto risico te verlagen.

Informatiebeveiliging
Het verdient aanbeveling de toegang tot de informatie te beveiligen door encryptie en twee-factor-authenticatie. Op die manier wordt de kans verkleind dat onbevoegden de data kunnen benaderen en inzien. Ook is het van belang de toegang tot de data te beperken door te werken met een klein aantal geautoriseerde gebruikers die moeten inloggen met een gebruikersnaam en wachtwoord. Dat maakt het mogelijk achteraf altijd te achterhalen wie op welk moment is ingelogd. Door handelingen met de data te loggen, wordt het ook mogelijk te achterhalen wie wat met de data heeft gedaan.

Korte bewaartermijnen, automatisch verwijderen
Camerabeelden worden in veel gevallen 28 dagen bewaard, omdat dit ook de termijn is die voor andere camerasystemen geldt, zoals gemeentelijke camera's voor handhaving van de openbare orde of bodycams. Maar die bewaartermijn kan voor het uitvoeren van analyses sterk worden teruggebracht omdat de oorspronkelijke kentekens zelf niet nodig zijn. Daarom verdient het aanbeveling de analyses te doen op basis van een zo kort mogelijk bewaard databestand. Ook verdient het aanbeveling om geëxporteerde gegevens een "houdbaarheidsdatum" mee te geven waarna ze automatisch worden vernietigd.

ISO 27001
Door te werken met leveranciers van ANPR-camera's die gecertificeerd zijn volgens de NEN/ISO27001 kan volgens algemeen erkende normen worden gewerkt. Dergelijke bedrijven moeten om hun certificaat te behouden jaarlijkse controles uitvoeren om te beoordelen of hun systemen nog aan alle eisen voldoen. Dat gebeurt op basis van interne controles, maar ook door pen- en hacktesten te laten uitvoeren. Tevens zijn deze bedrijven in staat alle informatieverwerkingen te monitoren en acties te loggen waarover dan kan worden gerapporteerd aan de opdrachtgever.

Hashing
Een interessante optie om de privacy van betrokkenen te beschermen is hashing van de kentekens voordat ze worden gebruikt voor analyses. Dat wil zeggen dat het gelezen kenteken wordt omgezet in een andere code die niet meer kan worden herleid naar de oorspronkelijke cijfers en letters. Hashing is een eenrichtingsproces dat niet kan worden omgekeerd. Het wijkt dus af van encryptie, omdat die gegevens met de correcte decryptiesleutel weer kunnen worden ontcijferd naar het origineel. Als gegevens worden gehashd, blijft informatie onleesbaar, zelfs als er een datalek is. Dit is uiteraard alleen een optie als de kentekens niet hoeven te worden verrijkt met informatie uit andere databases.

4.3 Beschermingsmaatregelen: organisatorisch

Informeren betrokkenen
Het is belangrijk transparant te zijn over verwerkingen van persoonsgegevens. Als een gemeente ANPR-camera's plaatst voor de handhaving van bijvoorbeeld een milieuzone, Zero Emissie-zone of geslotenverklaring, moet daarover uiteraard al worden gecommuniceerd met betrokkenen. Dat geldt ook voor de analyses die op de verzamelde gegevens worden uitgevoerd. Conform de richtlijnen van de European Data Protection Board is het raadzaam informatie in twee lagen beschikbaar te stellen.

Fysieke informatie (eerste laag)
De eerste informatielaag moet fysiek zichtbaar zijn op straat: de camera's moeten zichtbaar zijn en er kan een sticker of informatiebord worden geplaatst. Volgens de European Data Protection Board moet de belangrijkste informatie worden geboden: niet alleen het feit dat er kentekens worden gescand, maar ook het doel van de verwerking (handhaving), wie de verwerkingsverantwoordelijke is (gemeente) en de belangrijkste informatie

over de verwerking (bewaartermijn, analyses). Tot slot moet er een link worden geboden waar mensen meer informatie online kunnen vinden.

Online informatie (tweede laag)
Op een website moet informatie over de analyses worden toegevoegd aan de (specifieke) privacyverklaring en het verwerkingsregister van de gemeente. Daar moet het voor iedereen waar een kenteken van is gescand duidelijk worden hoe zij hun rechten kunnen uitoefenen. Iedereen heeft in de AVG een aantal rechten gekregen, waaronder het recht op inzage. Mensen hebben het recht om te horen of iemand persoonsgegevens over hen verwerkt. Dat is het geval bij kentekenherkenning, dus de gemeente moet dit soort inzageverzoeken volgens de AVG kunnen afhandelen. Het recht op inzage geldt voor alle camerasystemen, dus het is logisch dit te regelen op het moment dat de kentekencamera's worden geplaatst. Dan is er geen extra werk nodig op het moment dat de gescande kentekens worden gebruikt voor analyses.

Screening van medewerkers en geheimhoudingsverklaringen
Door het aantal functionarissen dat toegang kan krijgen tot de informatie zo klein mogelijk te maken, wordt het risico op datalekken of andere problemen al flink verkleind. Maar degenen die wel toegang krijgen moeten zorgvuldig worden gescreend. Veel gemeentelijke medewerkers leggen hier een eed of belofte af en tekenen een geheimhoudingsverklaring. Voor externe leveranciers of analisten moeten dezelfde eisen worden gehanteerd.

Werkinstructie en training medewerkers
Iedereen die bij de informatie kan komen, moet in een werkinstructie kunnen vinden welke regels gelden en op welke wijze de gegevens mogen worden verwerkt. Ook is het vaak nodig de medewerkers van de gemeente die met het analyse-systeem van de leverancier gaan werken een gebruikstraining te geven, zodat zij weten hoe alles werkt en hoe zij kunnen zorgen dat de informatie goed wordt beveiligd. Daarbij is een periodieke herhaling vaak nodig en ook nieuwe medewerkers moeten dezelfde werkinstructie en training krijgen.

Verwerkersovereenkomst met leverancier
De verwerkingsverantwoordelijke gemeente moet in een verwerkersovereenkomst met de leverancier vastleggen dat de verwerking voldoet aan de eisen van de gemeente. Hier is een landelijke standaard voor beschikbaar bij de VNG. Onder andere de volgende zaken moeten worden vastgelegd in zo'n overeenkomst:

- De leverancier verwerkt persoonsgegevens uitsluitend overeenkomstig schriftelijke instructies van de verwerkingsverantwoordelijke;
- De leverancier zorgt voor passende technische en organisatorische maatregelen om de persoonsgegevens goed te beveiligen;
- In aanvulling hierop voert de leverancier aanvullende acties uit voor de beveiliging, namelijk interne controle audits, pen- en hacktesten, reviews, security scans, monitoring en logging, rapportages, risicoanalyses, risicobehandelplannen en evaluaties van beveiligingsmaatregelen om risico's te mitigeren;
- de leverancier verleent medewerking aan audits;
- de leverancier helpt de verwerkingsverantwoordelijke als een betrokkene een beroep doet op zijn rechten;
- personen die voor de leverancier werken moeten persoonsgegevens geheimhouden en tekenen een geheimhoudingsverklaring;
- de leverancier informeert de verwerkingsverantwoordelijke zo snel mogelijk over (vermoedelijke) inbreuken in verband met persoonsgegevens, neemt zo snel mogelijk alle maatregelen en houdt een logboek bij;
- de leverancier zorgt ervoor dat persoonsgegevens niet buiten de Europese Economische Ruimte komen.

Periodieke controles of audits
Een gemeentelijke medewerker of een externe auditor moet periodiek controleren (bijvoorbeeld elke zes maanden) of alles nog werkt zoals beschreven en afgesproken. Het is bijvoorbeeld een goed idee om te controleren of informatie die moest worden verwijderd ook daadwerkelijk is verwijderd: sommige opslagsystemen zetten automatisch bestanden terug na een storing of bij een update van de software. Ook is de bewaartermijn soms langer dan afgesproken, omdat data pas worden verwijderd als de schijf vol is. Er moet ook een controle zijn op de autorisaties van de functionarissen die kunnen inloggen. Tot slot moeten alle logfiles

periodiek worden gecontroleerd om te zien wie heeft ingelogd en of dit inderdaad alleen geautoriseerde personen waren. Het is raadzaam de resultaten van dit soort audits te delen met de Functionaris voor Gegevensbescherming (FG).

Toezicht – door FG

De gemeentelijke Functionaris voor Gegevensbescherming houdt toezicht op naleving van de AVG. Het verdient aanbeveling in de Data Protection Impact Assessment expliciet op te nemen dat de FG aangekondigd en onaangekondigd controles mag uitvoeren op alle locaties en in alle systemen waar persoonsgegevens worden verwerkt om te beoordelen of de gemaakte afspraken worden nageleefd. De FG geeft na die controles advies aan de verwerkingsverantwoordelijke over eventuele issues en nieuwe privacy risico's. De reactie op dat advies wordt schriftelijk vastgelegd.

ANPR-camera’s gebruiken voor analyses; Juridisch advies

Onderzoek uitgevoerd door
Sander Flight – Onderzoek & Advies
Dimitri Pouwels – Pouwels Advies en Ondersteuning / RHDHV
Tess van den Blink – Privacy Management Partners

In opdracht van
Samenwerkingsproject Expertpool Stadslogistiek (SPES)
Ministerie van Infrastructuur en Waterstaat

Datum
30 januari 2024