VEXPAN
PLATFORM PARKEREN NEDERLAND

Vexpan Expertteam vraag: 2017-010

Aanvraag ingediend door : bestuur Vexpan
d.d. : februari 2017
Beantwoord d.d. : 15 januari 2018
Door ` : Goudappel Coffeng / Spark

Aanleiding

Kentekenregistratie bij betaald parkeren (op straat en in parkeergarages) en privacy zijn onderwerpen die als gevolg van de toenemende digitalisering in het parkeren actueel zijn en ook blijven. In 2015 is het Expertteam ingegaan op de belangrijkste aandachtspunten. De introductie van de nieuwe privacywetgeving in mei 2018 is een goede aanleiding weer opnieuw aandacht te besteden aan dit onderwerp, dit keer door in te gaan nieuwe Europese 'Algemene verordening gegevensbescherming'.

Nieuwe Europese wetgeving voor alle lidstaten

In 2016 is de nieuwe Europese richtlijn opgesteld voor bescherming en omgang van persoons- en privacygevoelige data welke uiteindelijk in 2018 geldend wordt. Vanaf 25 mei 2018 wordt hiermee de huidige 'Wet bescherming persoonsgegevens' (Wbp) vervangen door de 'Algemene verordening gegevensbescherming' (AVG). Binnen de EU hebbende lidstaten op dit moment elk een eigen privacywet; allen gebaseerd op de Europese privacyrichtlijn uit 1995. Deze richtlijn is verouderd en niet meer toereikend voor de huidige tijd. Naast de AVG wordt ook een uitvoeringswet AVG opgesteld. In de uitvoeringswet worden de nationale regels vastgelegd voor de uitvoering van de AVG binnen het specifieke lidstaat. De uitvoeringswet voor Nederland is op dit moment nog niet vastgesteld. Wel is hiertoe een conceptwetsvoorstel opgesteld.

Betere borging van rechten

Met de AVG wordt geborgd dat de rechten en bescherming van persoonsgegevens beter worden geborgd. Daarnaast wordt met de AVG de privacywetgeving binnen de alle EU-lidstaten gelijkgetrokken. De AVG biedt op een aantal punten ruimte voor de lidstaten om zelf de regels nader te bepalen of in te vullen. De invulling binnen Nederland wordt vastgelegd in de Uitvoeringswet AVG. Deze is momenteel nog niet vastgesteld; de bevoegdheid hiertoe ligt bij de regering en het parlement.

Overgangsperiode

Vanaf 25 mei 2016 is voor de periode tot 25 mei 2018 is een overgangsperiode ingesteld waarbinnen organisaties in staat worden gesteld om zich voor te bereiden op de AVG. Tot de inwerkingtreding van de AVG is de huidige Wet Bescherming Persoonsgegevens in Nederland nog van kracht.

Toepassing op de parkeersector: nog geen volledig en eenduidig beeld

Over de impact van de nieuwe wetgeving op gebied van kentekenparkeren bestaat vooralsnog geen eenduidig beeld. De praktische invulling van de wetgeving en bepaling van uitzonderingen zijn op dit moment inhoudelijk nog volop in ontwikkeling. Ook jurisprudentie zal zich nog moeten ontwikkelen om wetgeving te kunnen duiden. Op dit moment is hierdoor nog geen volledig inzicht in welke nieuwe taken en verantwoordelijkheden als gevolg van de AVG voor de verschillende typen organisaties binnen de parkeersector verplicht worden gesteld.

Context van het gebruik van de data is essentieel

Een belangrijke vraag die hier meer duidelijkheid in zal verschaffen, is hoe uiteindelijk binnen (de regelgeving van) de EU wordt omgegaan met de vraag óf, en zo ja in welke context, een kenteken valt onder privacygevoelige data of persoonsgegevens. In Duitsland wordt daar bijvoorbeeld op dit moment veel strenger mee omgegaan dan in Nederland. Aan de hand hiervan kan worden bepaald wanneer welk type organisaties en onder welke condities (gedeeltelijk) onder de

invloedssfeer van AVG vallen. Verwacht wordt dat met name het **type data** (bijvoorbeeld kenteken versus aanvullende data, mate van anonimiteit), **de verwerkingsprocessen** (bijvoorbeeld versleuteling van kentekens, toegankelijkheid) en het **type organisatie** (in hoeverre is deze in staat om een directe koppeling te maken tussen kenteken en individuele natuurlijke personen) en **het doel** van het gebruik van de data (toepassing van handhaving & toezicht, verkeersmanagement of commerciële doeleinden) uiteindelijk bepalend gaan worden. Door verdere aanscherping van de AVG vanuit de EU, nieuwe inzichten en jurisprudentie zal uiteindelijk een eenduidig eindbeeld moeten ontstaan.

Relevant voor partijen in de (digitale) parkeerketen

Verwacht wordt dat de AVG uiteindelijk in meer of mindere mate relevant wordt voor nagenoeg iedere organisatie die gebruik maakt van een systeem van (min of meer) gedigitaliseerde parkeerhandeling(en). Hierbij valt te denken aan, in ieder geval, organisaties in de parkeerketen die te maken hebben met handhaving of de afhandeling van bijvoorbeeld de parkeertransactie; zoals belparkeren, kentekeninvoer bij een parkeerautomaat, houders van vergunningen c.q. een digitaal parkeerrecht, toepassing van apps of andere platformen en inrijden in een parkeergarage met kentekenherkenning. Vanwege de digitalisering van het parkeren kan gesteld worden dat de AVG dus relevant wordt voor een aanzienlijk deel van de organisaties die actief zijn binnen de parkeerwereld.

*A**dvies Autoriteit Persoonsgegevens. I**n oktober 2017 is vanuit het Expertteam contact gezocht met de Autoriteit Persoonsgegevens (AP) over de laatste stand van zaken binnen de AVG. Voorliggend document geeft de laatste stand van zaken weer. In hoog tempo wordt steeds meer duidelijkheid over de AVG en de invulling en uitvoering hiervan. De AP communiceert op haar website de laatste stand van zaken en ontwikkelingen. De AP raadt aan om deze website nauwlettend in de gaten te houden. Bedrijven en organisaties die de website frequent controleren op updates, en tijdig opvolging geven aan de beschreven nieuwe inzichten en activiteiten, zijn in mei 2018 volledig voorbereid en aangepast aan de nieuwe regelgeving.*

Daarnaast is de positie van een kenteken in de nieuwe regelgeving besproken. Op dit moment verschilt de positie van kentekens en de mate van (persoonsgevoelige) informatie tussen de verschillende lidstaten. Met de AVG wordt binnen alle lidstaten uiteindelijk dezelfde regelgeving van kracht. Het is op dit moment nog niet duidelijk wat de positie van kentekens binnen de AVG wordt en wat de consequenties hiervan zijn voor de Nederlandse situatie. De AP heeft aangegeven dit vraagstuk op te volgen. Zodra hier inzicht in is, wordt gecommuniceerd op de "Vraag en Antwoord" pagina op haar website. De AP kan op dit moment nog niet aangeven wanneer ze verwacht de vraag te hebben beantwoord.

Meer rechten voor betrokken en meer verantwoordelijkheden voor organisaties

Op hoofdlijnen is inmiddels bekend wat de veranderingen van de AVG zijn ten opzichte van de huidige Wet bescherming persoonsgegevens. Zowel voor betrokkenen als voor organisaties die te maken hebben met privacygevoelige informatie, waaronder wellicht dus ook kentekens, verandert met de nieuwe situatie een aantal zaken. Onderstaand zijn de meest relevante veranderingen beschreven. Waar mogelijk is een doorvertaling gemaakt naar de impact op kentekenregistratie. Enkele organisaties zullen ook al ervaring hebben met een deel van de veranderingen.

Betrokkenen: versterking en uitbreiding van rechten

Personen van wie persoonsgegevens (zoals wellicht ook kentekens) worden bewaard, krijgen met de AVG meer rechten. Personen moeten met de komst van de AVG actief toestemming geven voor het verzamelen en verwerken van de data; het "standaard vinkje" volstaat in de toekomst niet meer. Hierbij dient deze persoon volledig en juist geïnformeerd te worden over onder andere welke data wordt bewaard, hoe lang deze wordt bewaard, met welk doel, wie inzicht hebben in de data en eventuele toestemming voor verstrekking van de gegevens. De verleende toestemming moet voor mensen net zo makkelijk in te trekken zijn als om die te geven. Daarnaast bestaat binnen AVG het recht om de gegevens te corrigeren of zelfs te laten verwijderen (recht op vergetelheid). Een laatste belangrijke verandering voor personen is het recht op

dataportabiliteit. Hiermee kan men de verzamelde data in een standaardformat opvragen voor bijvoorbeeld aansluiting bij een andere dienstverlener of eisen van de betreffende organisatie dat deze direct doorstuurt naar de nieuwe dienstverlener.

Organisaties: meer taken en verantwoordelijkheden

Voor organisaties die onder de werkingssfeer van de toekomstige AVG vallen, zal een aantal aspecten veranderen. Een grote verandering vindt plaats in de sancties bij overschrijding van de voorschriften uit de AVG. De boetes kunnen met de AVG oplopen tot 20 miljoen euro per overtreding of 4% van de (wereldwijde) omzet van een organisatie.
De Autoriteit Persoonsgegevens (AP) wordt binnen Nederland de toezichthoudende instantie op gebied van naleving van de AVG. De verwerking van persoonsgegevens hoeft met de AVG vanaf mei 2018 niet meer standaard te worden gemeld bij de Autoriteit Persoonsgegevens. Wel moet een organisatie desgevraagd verantwoording kunnen afleggen en aantonen aan de hand van documentatie. Voor organisaties met vestigingen in meerdere EU-lidstaten vindt een versimpeling plaats; onder de AVG hebben deze organisatie in de toekomst nog maar met één privacytoezichthouder van doen.

Anticiperen door organisaties: de zeven belangrijkste veranderingen

Organisaties kunnen op de komst van de AVG alvast voorsorteren door ervoor te zorgen dat de relevante mensen in de organisatie op de hoogte zijn van de nieuwe privacyregels en de veranderingen als gevolg van de nieuwe wetgeving. Door nu al een inschatting te maken van de impact van de AVG op de huidige processen, diensten en goederen kan snel inzicht verkregen worden welke aanpassingen nodig zijn om aan de nieuwe wetgeving te voldoen. Organisaties met vestigingen in meerdere EU-lidstaten kunnen alvast voor zichzelf bepalen onder welke privacytoezichthouder de organisatie vanaf 25 mei 2018 komt te vallen.

Onderstaand zijn de zeven inhoudelijk belangrijkste veranderingen uiteengezet:

1. **Verantwoordingsplicht.** Voor organisaties komt een verantwoordingsplicht. Hiermee worden organisaties verplicht op ieder moment een duidelijke en volledige verantwoording af te kunnen leggen over de wijze hoe de gegevens worden gewonnen en hoe met de gegevens wordt omgegaan. De verwerkingsprocessen dienen nauwkeurig te worden geadministreerd zodat een toezichthouder kan controleren of verplichtingen vanuit de AGV in de praktijk daadwerkelijk worden nageleefd. Hierin wordt ook aangegeven hoe onderstaande punten zijn meegenomen.

   Organisaties kunnen hierop nu al voorsorteren door te starten met het op orde krijgen van de benodigde documenten. Breng de processen en gegevensverwerkingen van (camera)registratie van kentekens tot betaling en handhaving tot uiteindelijke verwijdering van de data in kaart. Documenteer hierbij op een transparante manier welke gegevens worden verwerkt, met welk doel, met wie deze worden gedeeld, et cetera. Stel deze overzichten alvast dermate op dat deze op een later moment kunnen worden gebruikt als verantwoording aan de toezichthouder.

2. **Informatieverplichting.** Organisaties krijgen binnen de AGV de verplichting om meer en duidelijker te communiceren omtrent de dataverzameling en -verwerking. Te denken valt hierbij aan doel van de verzameling, de periode waarvoor gegevens worden opgeslagen, de juridische grondslag, de verwerking van deze gegevens, de rechten van de betrokkene (bijvoorbeeld recht op dataportabiliteit), et cetera.

   Organisaties kunnen hierop nu al voorsorteren door het evalueren en opstellen van een transparant inzicht in de rechten van betrokkenen (personen van wie (kenteken)gegevens worden bewaard) en een juiste borging van deze rechten. Dit geldt zowel voor bestaande rechten als voor nieuwe rechten (bijvoorbeeld dataportabiliteit). Ook de wijze waarop de organisatie toestemming vraagt, krijgt en registreert voor de verzameling en verwerking van persoonsgegevens kan alvast inzichtelijk worden gemaakt. Sta hierbij ook alvast stil over hoe en waar de organisatie deze informatie wil gaan communiceren.

3. **Meldplicht datalekken.** Organisaties zijn verplicht om alle datalekken te documenteren en een overzicht van alle datalekken bij te houden. De toezichthouder kan organisaties verzoeken om inzage in deze administratie te verschaffen en hiermee dus ook controleren of aan de meldplicht is voldaan. De AVG stelt verplicht om wanneer het “waarschijnlijk is dat de inbreuk resulteert in een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van

persoonsgegevens of de rechten en vrijheden van natuurlijke personen" zo snel mogelijk, zonder onnodige vertraging, te melden aan toezichthouders. Ook de personen van wie gegevens zijn verzameld dienen direct op de hoogte worden gesteld van het datalek.

Organisaties kunnen hierop nu al voorsorteren door actieplannen te ontwikkelen, testen en implementeren betreffende hun optreden in het geval van datalekken en crisissituaties.

4. **Data Protection Officer (DPO).** Een aantal organisaties is verplicht een Data Protection Officer (DPO) aan te stellen. Deze houdt toezicht op de toepassing en naleving van de AVG binnen de organisatie, waaronder ook de bescherming van gegevens, en fungeert als intern en extern aanspreekpunt op het gebied van gegevensverwerking en -bescherming. Iedere organisatie is vrij een DPO aan te stellen. Een DPO is verplicht voor in ieder geval:
   - Publieke organisaties en overheidsinstanties of -organen
   - Organisaties die als kernactiviteit hebben een reguliere, systematische of grootschalige controle van personen (bijvoorbeeld door middel van camera's of voertuigvolgsystemen);
   - Organisaties die krachtens een nationale wet een DPO moeten aanstellen.

   Organisaties kunnen hierop nu al voorsorteren door te bepalen in hoeverre de organisatie in de toekomst verplicht wordt om een DPO aan te stellen. Mocht een organisatie hiertoe verplicht zijn dan is het van belang te zorgen voor een tijdige werving en opleiding van de DPO.

5. **Data Protection Impact Assessment (DPIA).** Sommige organisaties krijgen de verplichting een DPIA uit te voeren. Hierin worden vooraf de privacyrisico's van de gegevensverwerking in beeld gebracht. Aan de hand van de DPIA kan de organisatie vervolgens maatregelen opstellen om de risico's, van bijvoorbeeld datalekken, te verkleinen. Een DPIA is verplicht als de gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de mensen van wie de organisatie gegevens verwerkt. Dit geldt in ieder geval voor organisaties die:
   - systematisch en uitvoerig persoonlijke aspecten evalueren;
   - op grote schaal bijzondere persoonsgegevens verwerken;
   - op grote schaal en systematisch mensen volgen in openbare en publiek toegankelijke ruimtes (bijvoorbeeld met cameratoezicht)

   Organisaties kunnen hierop nu al voorsorteren door in te schatten of de organisatie verplicht wordt om een DPIA uit te voeren. Dit is vooralsnog vrij lastig doordat nog geen concreet inzicht in welke definitie wordt gehanteerd voor bijvoorbeeld "systematisch" of "op grote schaal" alsook de relatie tot kentekenregistratie. Als blijkt dat de organisatie verplicht is om een DPIA uit te voeren dan wordt aanbevolen ook alvast maatregelen voor de benodigde risicobeperking op te stellen.

6. **Voorwaarden data.** Organisaties worden geacht om de verwerking van gegevens zodanig te organiseren dat uitsluitend noodzakelijke gegevens worden verzameld, bewerkt en bewaard. De data mag uitsluitend worden verwerkt voor het beoogde doel en ook niet langer worden bewaard dan strikt noodzakelijk. Het is aan de organisatie zelf om vooraf de criteria en onderbouwing voor het vaststellen van de bezwaartermijn te bepalen.
   Organisaties dienen ook passende maatregelen te nemen om de gegevensbescherming te waarborgen. Deze kunnen bijvoorbeeld worden gedefinieerd uit de Data Protection Impact Assessment. Een van de mogelijk te treffen maatregelen is pseudonimisering; waarmee persoonsgegeven zodanig worden verwerkt dat geen directe herleiding plaats kan vinden naar een individu zonder tussenkomst van aanvullende, afzonderlijk opgeslagen informatie. Hiermee worden gegevens anoniem en vallen buiten de verdere werkingssfeer van de AVG.

   Organisaties kunnen hierop nu al voorsorteren door vertrouwd te raken met de onder de AVG verplichte uitgangspunten van 'privacy by design' en 'privacy by default' en na te gaan hoe deze beginselen binnen de organisatie kunnen worden ingevoerd. 'Privacy by design' houdt in dat al bij het ontwerpen van producten en diensten zorg wordt gedragen voor de goede bescherming van de persoonsgegevens. Hierbij valt te denken versleuteling van kentekens en eventuele aanvullende (betaal)data, apps, afgeschermde (digitale) omgeving waar de data wordt bewaard, beveiliging van camerasystemen en wie heeft toegang tot de data.

'Privacy by default' houdt in dat technische en organisatorische maatregelen worden getroffen om ervoor te zorgen dat de organisatie, als standaard, alléén die persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat de organisatie wilt bereiken. Een organisatie dient zich dus af te vragen in hoeverre kentekengegevens daadwerkelijk nodig zijn (zijn er alternatieven?), welke aanvullende informatie (bijvoorbeeld persoonsgegevens, tijdstip, locatie, betaalgegevens) is écht noodzakelijk en wat is de uiterste minimale bewaartermijn die nodig is?

7. **Verplichtingen voor verwerkers.** Voor verwerkers (derden) van data schrijft de AVG een aantal directe verplichtingen voor. Aanvullend op deze directe verplichtingen dient een reeks contractuele waarborgen te worden opgesteld die een organisatie dient te treffen alvorens een verwerker in te schakelen. Hierin wordt onder andere geheimhouding, teruggave en/of vernietiging van persoonsgegevens en de uitvoering van audits opgenomen.

Organisaties kunnen hierop nu al voorsorteren door te inventariseren in hoeverre de overeengekomen maatregelen in bestaande contracten met derden (bewerkers) nog toereikend zijn en voldoen aan de criteria uit de AVG. Daar waar noodzakelijk moeten deze tijdig worden herzien en geactualiseerd.

De parkeerketen: wie neemt het voortouw?

Kennisdeling is gewenst

Zeker is dat met de komst van de AVG gaat ook binnen de parkeersector een verschuiving in de bevoegdheden, taken en verantwoordelijkheden plaats gaat vinden. Hoewel in de basis de AVG een zaak is van iedere organisatie 'an sich', liggen binnen Vexpan uitstekende mogelijkheden hierop in te spelen voor de gehele parkeersector. Vexpan kan een toegevoegde waarde bieden door (het faciliteren van) kennisdeling (zowel via bijeenkomsten en via de website) en het stimuleren dat leden de best practices van uniforme maatregelen, processen en/of documenten waarmee een correcte naleving van de AVG wordt geborgd, met elkaar delen zodat deze breed door de hele sector toegepast kunnen worden. Voorbeelden waaraan gedacht kan worden is het opstellen en delen van uniforme kaders voor dataportabiliteit, privacy by default en privacy by design, verplichtingen voor verwerkers en protocollen voor documenteren en informeren.

Bundeling van de reeds bestaande kennis en ervaring biedt een vertrekpunt voor een sectorbrede borging van de AVG in protocollen en uitvoering. Bijkomend voordeel is dat dit inzicht geeft in kansen en mogelijkheden voor verdere optimalisering van service en digitalisering van parkeren. Een verder gaande optie is om op korte termijn in projectgroep verband met betrokken partijen opdrachtgevers, opdrachtnemers en anderen te komen tot bijvoorbeeld een aantal standaarden/kaders en controle protocollen. Dat beperkt het steeds opnieuw uitvinden van het wiel door exploitanten, leveranciers en anderen en is voor alle betrokkenen efficiënt.

Kennis binnen leden Vexpan aanwezig

Binnen Vexpan en haar leden is de benodigde kennis en ervaring hiervoor waarschijnlijk deels al aanwezig. Enkele organisaties binnen de parkeerbranche hebben inmiddels, in meerdere of mindere mate, ervaring opgedaan met de veranderende verantwoordelijkheden zoals die verplicht worden gesteld met de komst van de AVG. Bijvoorbeeld vanuit hun huidige rol of naar aanleiding van juridische trajecten. Zo hebben bijvoorbeeld gemeenten ervaring op gebied van privacy aan leveranciers van onstreet en offstreet parkeerapparatuur en ICT-systemen, heeft RDW enige ervaring met privacy by default en privacy by design en heeft SHPV inzicht in de (huidige) verplichtingen voor verwerkers op gebied van privacy.
Overige stakeholders binnen de parkeersector kunnen leren van de opgedane ervaringen en lessons learned van deze organisaties. Dit biedt enkele voordelen. Zo is de opzet al gespecifieerd naar het thema parkeren en wordt efficiënter ingespeeld op de veranderingen als gevolg van de AVG doordat dubbel werk wordt voorkomen (niet iedere organisatie hoeft opnieuw 'het wiel uit te vinden'). Aanvullend hierop wordt geleerd van andermans fouten waardoor valkuilen kunnen worden vermeden en schade in het draagvlak en aanzien van de parkeersector wordt voorkomen.

Autoriteit Persoonsgegevens als klankbord

De Autoriteit Persoonsgegevens (AP) wordt binnen Nederland zogezegd de toezichthoudende instantie op gebied van naleving van de AVG. Vanuit haar huidige en toekomstige rol is de AP ook gedurende de implementatiefase van AVG bij twijfel benaderbaar als raadplegend orgaan of klankbord.

Mogelijkheden doorontwikkeling van data en informatie met behulp van kentekens

Zowel in Nederland als in de omringende landen is het gebruik van kentekens voor velerlei doeleinden in opkomst. Het gebruik van kentekens biedt niet alleen voor controle en handhaving kansen, maar ook, ontdaan van eventuele koppelingen met persoonsgegevens, een schat aan mogelijkheden om slimmer, efficiënter en beter onderzoek te doen en is daarmee haast onontbeerlijk voor *smart cities*. De vraag is daarom gerechtvaardigd wat wel kan en waar kansen liggen voor de nabije toekomst; zowel juridisch als technisch.

Het doel heiligt de middelen

Privacybescherming van de burger staat zoals beschreven hoog in het vaandel van Europese regelgeving. In Nederland zijn echter ook nog de beginselen van proportionaliteit en subsidiariteit aan de orde. Proportionaliteit wil zeggen: staat belang in verhouding tot de inbreuk? Bij subsidiariteit stellen wij ons de vraag: is dit de beste manier om het te bereiken? Of zijn er nog andere manieren?
Bij de beoordeling van proportionaliteit en subsidiariteit moet sprake zijn van een hoger doel. Bijvoorbeeld het bereikbaar houden van de stad. De vraag is vervolgens of het gebruik van parkeerdata ten behoeve van onderzoek of uitvoering van overheidstaken proportioneel in verhouding tot een beperkte schending van de privacy. Is sprake van de behartiging van een gerechtvaardigd belang van de verantwoordelijke. Met andere woorden: heiligt het doel de middelen? Bijvoorbeeld ten behoeve van een onderzoek naar de herkomst van parkeerders op een bedrijventerrein om op basis van de data te bezien wat de mogelijkheden zijn voor het toepassen van mobiliteitsmanagement en MaaS-oplossingen.

Ook de nut en noodzaak van een digitale parkeerketen kan zo worden beschouwd. Bij de invoer van een kenteken op de automaat heeft de rechter de volgende conclusie getrokken: het invoeren van een kenteken is – in verhouding tot het doel: een efficiëntere uitvoering van de handhaving – een beperkte aantasting van de privacy. De klant is gebaat bij de invoering van een kenteken op de automaat omdat men niet meer heen en weer hoeft te lopen van automaat naar auto om het ticket neer te leggen (gemaksaspect). En het is niet meer mogelijk om een ticket door te geven aan een andere bestuurder aangezien deze op kenteken staat (voorkomen van frauduleus handelen).

Ook buiten Nederland is daarbij de discussie omtrent privacy gaande. En niet zelden is de regelgeving daar strikter dan in ons land. Zo valt bijvoorbeeld in Duitsland kentekenregistratie in parkeergarages onder de “Datenschutz” wetgeving, waarvan de interpretatie per Bundesland verschilt. In Kopenhagen worden weliswaar kentekens voor de handhaving met behulp van een scanvoertuig geregistreerd, maar is het uit den boze dat omgevingscamera’s ook maar enig beeld maken van de feitelijke plaats en positie van het voertuig waardoor de bruikbaarheid beperkt is. In het algemeen kan gesteld worden dat ook internationaal jurisprudentie nog in ontwikkeling is, maar dat vooral de grote gevoeligheid in kentekendata zit in de combinatie met (nauwkeurige) geografische data. Juridisch is het nodige mogelijk, maar oplettendheid is op z’n plaats.

Welke kansen zijn er voor het genereren van betere of zuiverdere informatie uit de parkeerdata?

Bij de meeste onderzoeken is de overheid of een garage-exploitant niet geïnteresseerd in het gedrag van de individuele automobilist of parkeerder, maar om een representatief beeld te hebben van het feitelijke gebruik door groepen automobilisten met dezelfde kenmerken.

1. **Traditioneel onderzoek maar dan veel beter en efficiënter.** Parkeerdrukmetingen, parkeerduuronderzoek en doelgroepsegmentatie wordt traditioneel handmatig uitgevoerd. Tellers worden periodiek de straat op gestuurd om het aantal auto’s te tellen (parkeerdruk), een (globaal) inzicht te kregen in wie er parkeert (door op verschillende maatgevende momenten te tellen of door kentekens te registreren en deze door het RDW te laten segmenteren naar postcodegebied) en hoelang de automobilist parkeert (door meerdere keren per dag de kentekens te noteren). Kentekens worden dus als sinds mensenheugenis voor onderzoeksdoeleinden gebruikt. Handmatige onderzoeken zijn echter kostbaar en worden daarom slechts in beperkte mate gehouden. Door zeer regelmatig alle kentekens te scannen is het mogelijk een nagenoeg continu onderzoek te houden waarin trends en ontwikkelingen direct zichtbaar worden.
2. **Herkomstonderzoek** van bezoekers wordt om vele redenen vaak toegepast op basis van enquêtes. Voor gerichte marketingcommunicatie wil een winkelcentrum weten wie de klanten zijn en waar ze vandaan komen. Voor dergelijke onderzoeken, maar ook voor de inrichting van parkeerzones (bijvoorbeeld in vergunninggebieden) kan informatie

worden verkregen door kentekens te relateren aan de postcode van de berijder. In deze gevallen is het wel zaak om te onderzoeken of sommige postcodegebieden alsnog niet van zo'n omvang zijn dat herleiding naar een persoon mogelijk is.

3. **Frequentieonderzoek** Hoe vaak iemand ergens parkeert wordt zelden onderzocht. Met kentekenonderzoek is dat eenvoudig mogelijk als kentekens voor een langere periode worden bewaard.
4. **Segmentering op basis van kenmerken van het voertuig.** Voor onderzoek kunnen voertuigkenmerken relevant zijn, zoals bijvoorbeeld als men de milieubelasting van het autogebruik in een bepaald gebied wil bepalen. Zonder koppeling met de eigenaar van de auto zijn onder andere merk en type, milieuklasse, ouderdom en de catalogusprijs beschikbaar.

Bij het gebruik van kentekendata moeten afspraken worden gemaakt met alle leveranciers: die van de scanapparatuur/backoffice, parkeerrechtendatabase en vergunningensysteem. Afspraken over data encryptie, bewaartermijnen en vernietiging van gegevens. In de huidige praktijk blijkt dat deze afspraken vaak wel gemaakt worden, maar dat systemen – als het puntje bij het paaltje komt - niet als zodanig zijn ingesteld en, erger nog, niet instelbaar blijken te zijn. Daarom zijn tussentijdse audits, maar ook pre-tests in dit soort onderzoekssituaties van groot belang. Een datalek zit in een klein hoekje.