Introductie

Onderstaand treffen jullie de tweede versie van de vraagbaak van de community juridische aspecten. Deze richt zich in eerste instantie op de ontwerpers en exploitanten van Smart mobility diensten. De indeling is iets veranderd: de checklist uit de vorige versie is gewoon als vraag en antwoord opgenomen. De bedoeling is dat de vraagbaak verder zal worden gevoed vanuit de contacten met de projecten. Mocht u vragen hebben over de juridische aspecten van Smart Mobility dan kunt u de per e-mail zenden naar ***generiek emailadres?***, of bellen naar Wouter van Haaften, 06 107 23 500.

Vraag en Antwoord

Update datum: *november 2017*

Inleiding

Dataprotectie is geen exacte wetenschap, de wettelijke bepalingen vergen altijd een zekere mate van interpretatie bij het toepassen in een concreet geval. Absolute zekerheid over de juiste interpretatie is vaak vooraf niet te krijgen, maar onder de nieuwe Algemene Verordening Gegevensbescherming (AVG) die 25 mei 2018 van kracht wordt zijn de sancties dermate verhoogd (max. 4% van de wereldwijde jaaromzet) dat de meeste bedrijven geen risico's zullen willen nemen en nu echt serieus naar hun dataverwerking zullen gaan kijken. De AVG is rechtstreeks in de lidstaten van toepassing en hoeft dus niet in nationale wetgeving te worden verwerkt. Doel van deze Q&A is mede het bewustzijn en de handelingsmogelijkheden van alle spelers bij het verwerken van persoonsgegevens te vergroten. Deze Q&A gaat uit van de situatie na inwerking treden van de AVG en is verder is aangepast in verband met jurisprudentie van het EU Hof van Justitie.

Spelers

In de AVG definieert de volgende spelers bij de verwerking van persoonsgegevens:

Betrokkene: de natuurlijke persoon wiens gegevens worden verwerkt,[1]

Verwerkingsverantwoordelijke: degene die overgaat tot de verwerking van persoonsgegevens in het kader van zijn activiteiten en daarmee doel en middelen van de verwerking bepaalt,

Verwerker; degene die, ten behoeve van de verwerkingsverantwoordelijke, persoonsgegevens bewerkt.

De nieuwe AVG geldt voor zowel burgers, bedrijven als overheden.

Persoonsgegevens

Vraag:

- Hoe weet ik of ik persoonsgegevens verwerk?

De concrete vraag die daarbij hoort is: wat zijn persoonsgegevens? Dat zijn in de eerste plaats gegevens die, direct of indirect, bijvoorbeeld via het combineren van data, kunnen worden herleid tot een natuurlijk persoon?

Bijvoorbeeld: voertuigidentificatiegegevens (Voertuig Id Nummer en kenteken) worden als persoonsgegeven beschouwd, omdat zij via het kentekenregister in veel gevallen aan een natuurlijk persoon kunnen worden gekoppeld. Als er geen sprake is van persoonsgegevens dan is de Wet bescherming persoonsgegevens (Wbp) en vanaf 25 mei 2018 de AVG niet van toepassing.

[1] Strikt genomen geeft de AVG geen definitie van betrokkene. Wat onder 'betrokkene' moet worden verstaan volgt uit de definitie van 'persoonsgegevens'.

In de AVG is het begrip persoonsgegevens uitgebreid. Locatiegegevens worden expliciet als persoonsgegevens aangemerkt. Bovendien is door de Europese Autoriteiten Persoonsgegevens in het kader van de AVG[2] een interpretatie van het begrip persoonsgegevens gekozen die ertoe leidt dat het niet meer van belang is of iemand uiteindelijk geïdentificeerd zal kunnen worden. Ook als een anoniem persoon geïndividualiseerd (singled out) kan worden uit een groep, bijvoorbeeld een willekeurige weggebruiker op een bepaalde locatie, dan is het feit dat deze weggebruiker individueel benaderbaar is voldoende om de gegevens als persoonsgegevens aan te merken. Het is immers mogelijk om op die bepaalde locatie een locatie gebonden reclameboodschap aan de weggebruiker te zenden.

In feite komt het erop neer dat de verwerkte gegevens van een gepersonifieerde smart mobility app in beginsel als persoonsgegevens zullen moeten worden aangemerkt, tenzij kan worden aangetoond dat het individualiseren van personen absoluut niet mogelijk is.

Vraag:

- Is een kenteken op naam van een rechtspersoon, opgenomen met, bijvoorbeeld, een werknemer in de auto een persoonsgegeven.

Of een kenteken een persoonsgegeven is hangt af van verschillende factoren. Om te beginnen is van belang of aan het kenteken een persoon te koppelen is. Als het een werknemer van het bedrijf is en het bedrijf weet welke werknemer wanneer in welke auto zit, dan gaat het om een identificeerbaar gegeven, dus persoonsgegeven. Zo werd in de jurisprudentie het motornummer van een vliegtuig in het kader van een bepaalde vlucht als persoonsgegeven van de gezagvoerder aangemerkt. Daarnaast is van belang dat degene die het kenteken verwerkt ook feitelijk toegang heeft of kan krijgen tot de achterliggende persoonsgegevens, bijvoorbeeld via het kentekenregister. Private (rechts)personen hebben niet zo maar toegang tot de tenaamstellingslijst van het kentekenregister, overheidsinstellingen over het algemeen wel.

Gerechtvaardigde verwerking

Vraag:

- Hoe weet ik of er sprake is van een gerechtvaardigde verwerking?

De eerste stap die daarbij moet worden gezet is het beantwoorden van de vraag of de activiteit of dienst ook zonder de verwerking van persoonsgegevens kan worden uitgevoerd. Als dat het geval is dan mogen geen persoonsgegevens worden verwerkt.

Vraag:

- Wie beoordeelt of het verwerking gerechtvaardigd is?

In eerste instantie beoordeelt de verwerkingsverantwoordelijke dat, meestal degene die de dienst ontwerpt en in de markt zet. Deze geeft antwoord op de vraag of het mogelijk is de dienst te leveren zonder gebruikmaking van persoonsgegevens. Indien dit voor een dienst niet mogelijk is kunnen persoonsgegevens worden verwerkt. In dat geval moet een rechtsgrondslag worden bepaald op basis waarvan de persoonsgegevens kunnen worden verwerkt.

Rechtsgrondslag

Vraag:

- Hoe bepaal ik de rechtsgrondslag voor de verwerking van persoonsgegevens?

Persoonsgegevens mogen enkel worden verwerkt als daarvoor een geldige rechtsgrondslag bestaat. Dit kan bijvoorbeeld toestemming van de betrokkene zijn. Bij de meeste dienstverlening ligt het voor de hand om toestemming te vragen aan de betrokkene, die dan wel voordat hij/zij toestemming geeft voldoende geïnformeerd moet zijn. Niet alleen over de verwerking in het kader van de dienst, maar ook over eventuele verdere bewerkingen en leveringen van data die buiten het kader van de dienst vallen. Wanneer een verwerking berust op toestemming moet de verwerkingsverantwoordelijke achteraf kunnen aantonen dat hij toestemming heeft verkregen.

[2] Opinie 2/2017 van de WG art 29 over persoonsgegevens in C-ITS

Ook andere rechtsgronden zijn denkbaar maar omdat zij geen expliciete toestemming van de betrokkene omvatten zullen zij goed moeten worden onderbouwd om verrassingen achteraf te voorkomen. Voor dienstverlening valt te denken aan de verwerking in het kader van de uitvoering van een overeenkomst met de betrokkene, of verwerking in het geval dit in het gerechtvaardigd belang is van de verwerkingsverantwoordelijke. Voor deze laatste rechtsgrond is wel vereist dat een goede afweging wordt gemaakt van de belangen van de betrokkene ten opzichte van die van de verwerkingsverantwoordelijke (balancing test).

Verwerken

Verwerken in de zin van de AVG omvat alle behandelingen die de persoonsgegeven kunnen ondergaan. Zo is bijvoorbeeld ook het ontvangen of verzenden van persoonsgegevens een verwerking.

Vraag:

Aan welke voorwaarden moet de verwerking van persoonsgegeven voldoen?

Bij de verwerking van persoonsgegevens geldt een aantal wettelijke beginselen waaraan moet worden voldaan gedurende de verwerking van de persoonsgegevens:

- De verwerking moet rechtmatig, behoorlijk en transparant worden uitgevoerd. Er mogen niet meer gegevens worden verwerkt dan voor het doel nodig is (dataminimalisatie),
- Het doel van de verwerking moet zo helder en compleet mogelijk worden geformuleerd en duidelijk gecommuniceerd naar de betrokkene. Gegevens mogen niet voor andere doeleinden worden verwerkt,
- De omvang van de verwerking mag niet meer gegevens omvatten dan voor het doel noodzakelijk is,
- De gegevens moeten juist zijn en moeten eventueel door de betrokkene kunnen worden verbeterd,
- De duur van de verwerking mag niet langer zijn dan voor het doel noodzakelijk is,
- De gegevens moeten goed worden beveiligd, zowel technisch als organisatorisch, zodat de integriteit en betrouwbaarheid kan worden gegarandeerd,
- Beveiliging van de gegevens moet plaatsvinden volgens 'state of the art' technische standaarden tegen redelijke kosten, proportioneel aan het belang van de gegevensverwerking. Regelmatige aanpassingen zijn dus vereist. Zie ook de stukken bij de Smart Mobility community security; http://smartmobilitycommunity.eu/bibliotheek?f%5B0%5D=og_group_ref%3A21

Vraag:

Wat moet ik regelen als ik als verwerkingsverantwoordelijke niet zelf de persoonsgegevens verwerk, maar overlaat aan een verwerker?

In het geval de verwerkingsverantwoordelijke niet zelf verwerkt, maar dit opdraagt aan een verwerker moet met die verwerker een bewerkingsovereenkomst worden gesloten. Daarin worden de voorwaarden voor de bewerking door de verwerker vastgelegd. De verwerkingsverantwoordelijke blijft daarbij ten opzichte van de betrokkene verantwoordelijk. In de overeenkomst moeten, naast de rechtsgrondslag, ook de voorwaarden worden opgenomen waaronder de gegevens verwerkt mogen worden. Daarnaast moet de opdrachtgever eisen stellen met betrekking tot het naleven van de dataprotectiewetgeving. De verwerkingsverantwoordelijke blijft verantwoordelijk voor de bewerking door de verwerker.

Voorbeelden

Voorbeeld 1:

Een kenteken is pas een persoonsgegeven als deze te herleiden is tot een persoon.
In principe is deze relatie te leggen met behulp van de database van de RDW, waartoe niet iedereen toegang heeft. Een bedrijf dat kentekencamera's langs de weg heeft staan kan dus beweren dat de kentekens die zijn ingewonnen voor hen geen persoonsgegevens zijn, omdat zij die niet kunnen herleiden tot een persoon.

Vraag:

Klopt deze stelling?

Antwoord: Waarschijnlijk niet, zo blijkt o.m. uit jurisprudentie van het EU Hof van Justitie[3] in 2016. Als het in opdracht gebeurt van bijvoorbeeld RWS dan heeft RWS toegang tot het kentekenregister en zijn de gegevens al snel persoonsgegevens. Als het bedrijf de gegevens opneemt om gedurende een beperkte tijd verkeerstromen te volgen zonder de eigenaar/bestuurder te achterhalen en de gegevens vervolgens wist, is er alleen dan geen sprake van persoonsgegevens als redelijkerwijs verondersteld mag worden dat de voertuigen ook niet individualiseerbaar zijn geweest, hetgeen bij het beschikken over de combinatie kenteken/locatie onwaarschijnlijk is.

Voorbeeld 2:

Het spookfile project A-58 biedt een in car adviessnelheid waarmee bij een voldoende aantal deelnemers het collectieve rijgedrag zodanig kan worden beïnvloed dat gevaarlijke situaties door plotseling opkomende (spook)files kunnen worden vermeden. In ruil daarvoor verstrekken bedrijven uit de omgeving kortingen op producten, bijvoorbeeld een snack bij een benzinestation of een hamburger bij een wegrestaurant op de route. Er kan worden deelgenomen door opgave van een gebruikersnaam en emailadres. Het emailadres kan een voor dit doel aangemaakt Gmail adres zijn. De deelnemer hoeft dus geen enkel identificerend element op te geven aan de service- provider.

Vraag:

Is hier sprake van persoonsgegevens?

Antwoord: Uitgaande van het identificatiecriterium kon voorheen worden aangenomen dat als identificatie niet redelijkerwijs mogelijk is er geen sprake is van persoonsgegevens. De aanknopingspunten voor identificatie zijn: de smartphone van de deelnemer (de Telco), het Gmailadres(Google) en de fysieke verschijning als de deelnemer ingaat op een aanbieding van een lokale ondernemer (McDonalds). De mogelijkheden voor de serviceprovider om de identiteit van de deelnemer te achterhalen zijn echter te beperkt om de deelnemer te kunnen identificeren.

Het nieuwe criterium ‘single out’ houdt in dat als een voertuig, en dus de daarin aanwezige persoon, kan worden onderscheiden van andere voertuigen er sprake is van persoonsgegevens. In het geval van spookfiles is het wegrestaurant in staat om, op basis van de actuele locatiegegevens aan een deelnemer een min of meer gepersonaliseerde aanbieding te doen, bijvoorbeeld korting op de hamburger. Het feit dat de deelnemer het doelwit kan worden van deze advertentie op grond van de bekendheid van de locatie waar hij zich bevindt betekent, in de nieuwe opvatting van onder meer de dataprotectie autoriteiten, dat de gegevens op grond waarvan de aanbieding wordt gedaan als persoonsgegevens moeten worden aangemerkt. Dit ondanks het feit dat op grond van deze gegevens geen identificatie van de deelnemer mogelijk is.

Voorbeeld 3:

Hetzelfde bedrijf dat kentekencamera's langs de weg heeft staan werkt nu met bluetooth scanning. Hun systeem kan voertuigen tijdelijk volgen op basis van dit signaal en daarmee verkeersstromen in kaart brengen. Het systeem slaat de coördinaten niet blijvend op, maar ze blijven wel tijdelijk in het werkgeheugen van de server. Het bedrijf beweert dat het geen persoonsgegevens verwerkt omdat er geen relatie met het kenteken kan worden gelegd.

Vraag:

Klopt deze stelling?

[3] Zaak C-582/14, Patrick Breyer vs Bundesrepublik Deutschland 19 oktober 2016.

Antwoord: Nee, op zich zijn de locatiegegevens van een voertuig al persoonsgegeven, daar is geen identificerende slag via het kenteken voor nodig. Op basis van het bluetooth signaal is individualisering mogelijk. En overigens geldt ook hier: tijdelijke opslag is verwerken in de zin van de AVG.

Meldingsplicht

Vraag:

Wanneer en waar moet een verwerking van persoonsgegevens vooraf worden gemeld?

Antwoord: Verwerkingen moesten onder de Wbp in beginsel altijd vooraf aan de AP worden gemeld. Onder de AVG vervalt deze meldingsplicht maar is zowel de verwerkingsverantwoordelijke als de verwerker verplicht om een register bij te houden van alle onder hem gedane verwerkingen. De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van de AVG en moet dit desgevraagd kunnen aantonen. Om dat in het geval van externe verwerking te kunnen doen moet ook de verwerker aan deze verplichting voldoen. Vanaf 6 november 2017[4] wordt door de AP niet meer gehandhaafd, met uitzondering van de meldingen van risicovolle verwerkingen zoals bedoeld in art 31 Wbp en art 36 AVG.

Data-lek

De verwerker constateert een incident waarbij persoonsgegevens zijn gelekt.

Vraag:

Moet de verwerker het lek rechtstreeks melden bij de AP ?

Antwoord: Nee, bij de verwerkingsverantwoordelijke. Dit moet zo snel mogelijk gebeuren.

Vraag:

Volstaat dan een melding aan "de verwerkingsverantwoordelijke"?

Antwoord: Ja, het lek moet zo snel mogelijk bij de verwerkingsverantwoordelijke worden gemeld. onder vermelding van de aard van het lek, de naam van de contactpersoon, de gevolgen van de inbreuk en de maatregelen die zijn genomen om verdere gevolgen te beperken. De informatie mag ook in gedeelten worden verstrekt. De verwerker documenteert, mede ten behoeve van de verwerkingsverantwoordelijke, alle inbreuken in verband met de verwerking van persoonsgegevens.

Vraag:

Wat als de verwerkingsverantwoordelijke het incident vervolgens niet meldt bij de AP?

Antwoord: De verwerkingsverantwoordelijke moet vervolgens het lek binnen 72 uur melden bij de AP (art 33 AVG). Zo niet dan is de verwerkingsverantwoordelijke in overtreding, niet de verwerker.

Vraag:
Wanneer moet de verwerkingsverantwoordelijke een dergelijk lek melden aan de betrokkenen?

Antwoord: Verwerkingsverantwoordelijke dient de betrokkenen te informeren als een datalek waarschijnlijk ongunstige gevolgen heeft voor hun persoonlijke levenssfeer.

---

[4] https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/organisaties-hoeven-geen-melding-van-verwerking-gegevens-meer-te-doen