Datum: 24 juni 2016
Onderwerp: Concept Handreiking Verantwoordelijke in Consortia

Inleiding

Veel dienstverlening op het gebied van Smart Mobility wordt niet gerealiseerd door één dienstverlener. Vaak is er een keten van gespecialiseerde partijen die gezamenlijk de Smart Mobility dienst aanbieden. Daarbij zijn app-bouwers betrokken, infra service providers en data-leveranciers. En een dienstverlener die de dienst feitelijk aan de klant aanbiedt.

Bij deze dienstverlening worden gegevens van de klant gebruikt bij het samenstellen en het verlenen van de dienst. Als deze gegevens kunnen leiden tot identificatie van een persoon zijn ze aan te merken als persoonsgegevens. Zo worden bijvoorbeeld het voertuigidentificatienummer en het kenteken als persoonsgegevens aangemerkt. In het geval van een persoonsgerichte Smart Mobility dienst zal dus veelal sprake zijn van verwerking van persoonsgegevens en is de Wet Bescherming Persoonsgegevens (WBP) van toepassing. Deze wet schrijft voor hoe met persoonsgegevens moet worden omgegaan en wie daarvoor verantwoordelijk is.

Deze handreiking heeft tot doel te helpen bij het inrichten van deze verantwoordelijkheid binnen samenwerkingsverbanden, zoals consortia, die gezamenlijk een Smart Mobility dienst realiseren. Daarbij wordt ingegaan op de verschillende mogelijkheden om de verantwoordelijkheid in de zin van de WBP in te richten en op de relatie met de betrokkene. Aan de hand van deze handreiking kan de verantwoordelijkheid voor de verwerking van persoonsgegevens in een consortium eenduidig kan worden georganiseerd.

De Verantwoordelijke

De verantwoordelijke is de natuurlijke- of rechtspersoon of enig ander orgaan dat verantwoordelijk is voor de gegevensverwerking en die het doel (realiseren Smart Mobility diensten) en de middelen (geld, mensen, IT voorzieningen) van de verwerking bepaalt.
In deze wettelijke definitie bepaalt de verantwoordelijke:

- doeleinden van de gegevensverwerking;
- middelen voor de verwerking;

Naast deze wettelijke bepaling is aan de hand van de jurisprudentie ook een meer functionele benadering van het begrip verantwoordelijke ontstaan. Daarbij wordt meer gekeken naar feiten en omstandigheden zoals contractuele verhoudingen, de mate van zeggenschap van de verschillende partners en de zichtbaarheid voor de betrokkene.
De functionele benadering kijkt naar aanwijzingen zoals:

- welke gegevens worden door welke deelnemer verwerkt;
- welke deelnemer bewaakt de bewaartermijnen en vernietigt de gegevens;
- welke deelnemers hebben toegang tot de gegevens;
- welke deelnemer verstrekt informatie aan de betrokkene;
- welke deelnemer verstrekt eventueel persoonsgegevens aan derden binnen en/of buiten de EU.

Eén verantwoordelijke

De Wbp en de richtlijn gaan ervan uit dat de zeggenschap en bevoegdheden ten aanzien van de belangrijkste aspecten van dataverwerking meestal bij dezelfde natuurlijke of rechtspersoon liggen. Er is dan één verantwoordelijke die aangesproken kan worden op de verwerking van persoonsgegevens in het gehele proces.
De andere consortium-/ketenpartners kunnen in dat geval als verwerkers worden aangemerkt. Zij werken in opdracht van de verantwoordelijke. Verwerken is een ruim begrip, hieronder wordt verstaan het:

- verzamelen,
- vastleggen,
- ordenen,

- bewaren,
- bijwerken,
- wijzigen,
- opvragen,
- raadplegen,
- gebruiken,
- doorzenden,
- verspreiden,
- beschikbaar stellen,
- samenbrengen,
- met elkaar in verband brengen,
- afschermen,
- uitwissen
- vernietigen

van persoonsgegevens. Eigenlijk elke denkbare handeling die met de gegevens kan worden verricht. Een situatie waarbij sprake is van één verantwoordelijke schept voor zowel de consortiapartners als voor de betrokkene de meeste duidelijkheid. Het is aan de aanbieder van de dienst om naar diens afnemer, de betrokkene, helder te communiceren welke samenwerkings-/of ketenpartner de verantwoordelijke is. Onduidelijkheid over de identiteit van een verantwoordelijke kan niet aan de betrokkene worden tegengeworpen.

De Bewerker

Wanneer er sprake is van één verantwoordelijke dan worden bewerkingen van persoonsgegevens door de partners in het consortium verricht als bewerker. In dat geval is het aan de verantwoordelijke om contractuele afspraken te maken met de partners/bewerkers over de omgang met persoonsgegevens. Deze bewerkersovereenkomst moet een aantal punten specifiek regelen, bijvoorbeeld:
Het soort gegevens dat door de bewerker wordt bewerkt;
Het doel van de verwerking;
De termijn dat de gegevens mogen worden bewaard;
De beveiligingsmaatregelen die moeten worden genomen;
De geheimhoudingsplicht bevatten voor de bewerker en zijn personeel.

De Deelverantwoordelijke

Ook is denkbaar dat er afzonderlijke verantwoordelijkheden voor deelverwerkingen bestaan.
De betrokkene kan dan slechts de deelverantwoordelijke aanspreken in wiens deel van het proces de verwerking heeft plaatsgevonden. Omdat, zoals eerder gesteld, onduidelijkheid over de verdeling niet kan worden tegengeworpen aan de betrokkene stelt deze vorm binnen een consortium of keten heel hoge eisen aan de transparantie van de verwerkingen.

Gezamenlijke verantwoordelijkheid

Tenslotte kan het ook zo zijn dat de verwerkingen zodanig geïntegreerd dat er sprake is van een gezamenlijke verantwoordelijkheid.
Daarbij is ieder van de verwerkers hoofdelijk aansprakelijk jegens de betrokkene voor de goede verwerking van de gegevens, die dus ieder van de consortium-/ketenpartners kan aanspreken voor de verwerking van persoonsgegevens in het gehele proces.

Vooraf regelen

Het is zaak dat bij de start van een Smart Mobility dienst, betrokkenen een helder zicht moeten kunnen krijgen op wat er met hun persoonsgegevens gaat gebeuren.
Het is de taak van de verantwoordelijke hiervoor te zorgen; dit betekent dat de persoonsgegevens verwerking ruim vóór de start van het dienst bekend moet zijn. Ook de relaties met de partners in het consortium moeten dan ingeregeld zijn.

Sancties

Is dit niet het geval dan kan de Autoriteit Persoonsgegevens (voorheen College Bescherming Persoonsgegevens) een onderzoek starten. De eventueel op te leggen sancties zijn op dit moment nog zeer beperkt. De zwaarste 'sanctie' is de negatieve publiciteit en imagoschade die een dienstverlener of het consortium kan oplopen. Bij de komst van de nieuwe Algemene Verordening Data Protectie in 2018 kunnen echter boetes worden opgelegd tot maximaal 4% wereldwijde jaaromzet[1] van het overtredende bedrijf.

Rol Opdrachtgever

Omdat overheden vaak initiatiefnemer, opdrachtgever en/of facilitator van Smart Mobility projecten zijn, zal het voor kunnen komen dat betrokkenen vooral de betreffende overheid zien als verantwoordelijke, zeker als die (schijnbaar) grote bemoeienis heeft gehad bij de opzet van het project. In bepaalde gevallen kan de opdrachtgever zelfs als verantwoordelijke worden aangemerkt. Dit doet zich bijvoorbeeld voor als in de opdrachtformulering expliciet het gebruik van persoonsgegevens wordt voorgeschreven. In dat geval bepaald de opdrachtgever doel en middelen van de persoonsgegevensverwerking.

Privacy officer

In de nieuwe Verordening Data Protectie die in 2018 van kracht wordt is de verplichting opgenomen tot het aanstellen van een Privacy Officer. Dit is een onafhankelijke functionaris die direct onder het bestuur van de onderneming, of groep van ondernemingen valt, en die toezicht houdt op de naleving van de bepalingen uit de Verordening. De Privacy Officer hoeft niet per bedrijf te worden ingehuurd, maar kan ook op branche niveau of in een samenwerkingsverband worden aangesteld. De Privacy Officer is als het ware een vooruitgeschoven post van de Authoriteit Persoonsgegevens.

Uit de praktijk

A58 Spookfiles

Bij het project Spookfiles A58 werken bedrijven, overheid en kennisinstellingen samen aan spookfile-apps, gebaseerd op innovatieve Talking Traffic-technieken; deelnemende bestuurders krijgen adviezen om hun rijgedrag aan te passen aan de de verkeersituatie op een wegvak.
De hiervoor vanuit het voertuig gezonden data (via On Board Unit) bestaan onder andere uit een door de deelnemer zelf gekozen naam; echter door de daarmee ook uitgezonden locatie-informatie (tijdstippen gereden trajecten) zal echter toch snel sprake zijn van tot de persoon herleidbare en dus persoonsgegevens; daarmee is de Wbp van toepassing.

Wie is in deze constellatie de verantwoordelijke? Gelet op de onderlinge verhoudingen binnen een van de consortia, waarbij één partner doel en middelen van de verwerking bepaalt, zal deze ook als verantwoordelijke moeten worden aangemerkt.
De verzamelde gegevens zijn het e-mailadres en zelfgekozen naam en de geo-informatie die gedurende het gebruik van de app wordt verzameld. Met die informatie wordt verkeersadvies gemaakt en verzonden.
Naast de verantwoordelijke partner zijn nog twee andere partners betrokken: een dienstverlener die de gegevens tijdelijk opslaat en de app bouwer die niet betrokken is bij het maken en verzenden van het advies en dan ook geen toegang heeft tot persoonsgegevens. De verantwoordelijke heeft met de partner die data opslaat een bewerkersovereenkomst gesloten.

[1] Verordening (EU) 2016/679 van het Europees Parlement en de Raad, Artikel 83.

Voorbeeld 2, volgt

Innovatory/CGI,

Voorbeeld 3, volgt

Breda?

Vragenlijst

Persoonsgegevens:

Is er sprake van verwerking van persoonsgegevens? Kunnen de gegevens direct of indirect, bijvoorbeeld via het combineren van data, worden herleid tot een persoon? Bijvoorbeeld: voertuigidentificatiegegevens (VIN en kenteken) worden als persoonsgegeven beschouwd.

Als er geen sprake is van persoonsgegevens dan is de Wet Bescherming Persoonsgegevens niet van toepassing.

Doel:

Het verwerken van persoonsgegevens kan alleen met een legitiem doel. Dit moet helder geformuleerd worden en duidelijk worden gecommuniceerd naar de betrokkene.

Rechtsgrondslag:

Wat is de rechtsgrondslag voor de verwerking van persoonsgegevens? Bij de meeste dienstverlening ligt het voor de hand om uit te gaan van instemming van de betrokkene, die dan wel voordat hij/zij toestemming geeft goed geïnformeerd moet zijn. Ook andere rechtsgronden zijn denkbaar. Zij zullen echter goed moeten worden onderbouwd.

Wettelijke voorwaarden:

Als er sprake is van persoonsgegevens en er is toestemming van de klant of deelnemer, dan moet vervolgens nog aan een aantal voorwaarden worden voldaan gedurende de verwerking van de persoonsgegevens:

- Omvang van de verwerking mag niet groter zijn dan voor het doel noodzakelijk
- Duur van de verwerking mag niet langer zijn dan voor het doel noodzakelijk
- Beveiliging van de gegevens moet volgens heersende technische standaarden tegen redelijke kosten, proportioneel aan het belang van de gegevensverwerking.
- …

Checklist voor experts:

Op welke manier gaan jullie om met privacy?

Zijn de regels omtrent dataprotectie bekend?

Hoe is de samenwerking juridisch vormgegeven?

Zijn regels voor alle partners duidelijk?

Welke risico's ziet u?