# Privacy by Design en Smart Mobility

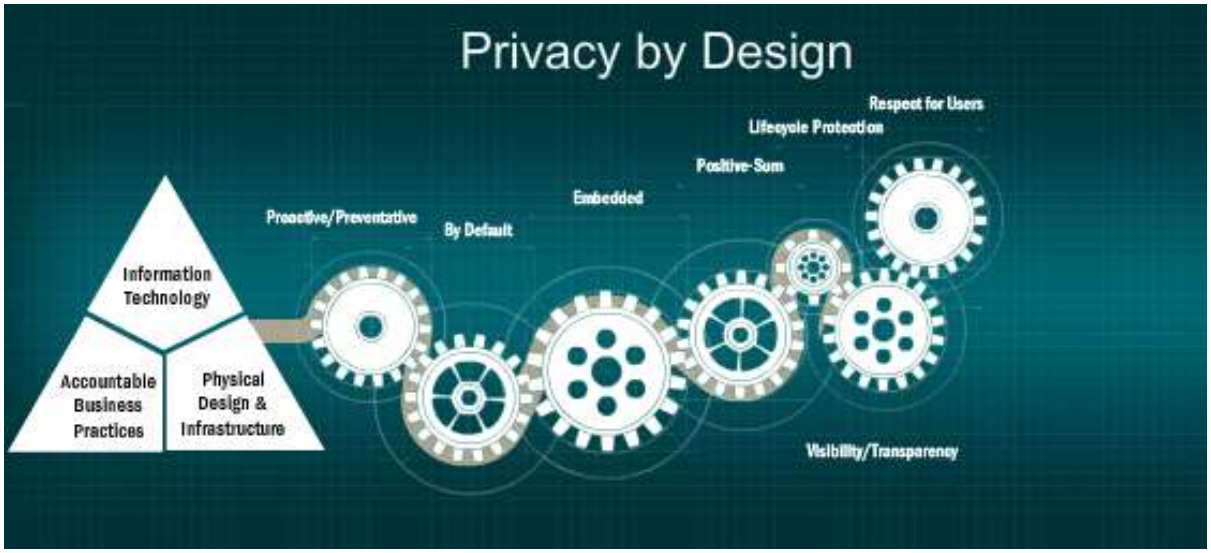
Wouter van Haaften

LANDELIJKE RONDE TAFEL VOOR SMART MOBILITY JURIDISCHE ASPECTEN

RONDETAFELS.DITCM.EU

# Privacy by Design en Smart Mobility

Op basis van de aankomende Europese Algemene Verordening Gegevensbescherming moet 'Gegevensbescherming door ontwerp' (Privacy by Design) worden toegepast in alle toepassingen waarbij persoonsgegevens worden verwerkt. Dit houdt in dat de bescherming van persoonsgegevens als standaard wordt gehanteerd in het ontwerp van IT systemen en bedrijfsprocessen, en in de inrichting van organisaties. Het nadenken over Privacy by Design moet dus beginnen zodra de contouren van een nieuwe Smart Mobility dienst zicht baar worden, en eigenlijk voordat 'de eerste spade de grond in gaat'.




## Inleiding

Deze handreiking levert geen blauwdruk voor de omgang met persoonsgegevens binnen Smart Mobility projecten. De handreiking biedt inzicht in het juridische kader van de bescherming van persoonsgegevens door middel van toelichting en voorbeelden. Daarbij wordt de noodzaak geïllustreerd om op alle onderdelen van de dienstverlening Privacy by Design toe te passen. Privacy by Design is een ontwerpbenadering en niet zozeer een concrete praktijk of technologie. Een bedrijf, organisatie of projectteam doet aan Privacy by Design wanneer bescherming van de privacy vanaf het vroegste ontwerp van een systeem wordt meegenomen, en deze aandacht voor privacy doorgaat gedurende de gehele levenscyclus van het systeem. Deze ontwerpbenadering van Privacy by Design gaat niet alleen over het gebruik van technologie, maar ook over de wijze waarop de organisatie wordt ingericht.

Privacy by Design is van toepassing bij het:

1. bepalen van de benodigde (persoons)gegevens set;
2. functioneel ontwerpen van de dienst;
3. het inrichten van de architectuur;
4. ontwerpen van de IT;
5. inrichten van de organisatie;
6. (juridisch) vormgeven van mogelijke samenwerking.

Kortom, bij aspecten van het ontwikkelen van de Smart Mobility dienst zal de vraag moeten worden gesteld: zijn de persoonsgegevens goed beschermd? Persoonsgegevens zijn alle gegevens die, direct of indirect tot een persoon te herleiden zijn. Zo zijn bijvoorbeeld naam en adres van een persoon direct herleidbare, en kenteken en IP-adres van een smartphone indirect herleidbare persoonsgegevens. Aangezien bij Smart Mobility diensten vaak bij de persoonsgegevens ook locatiegegevens van de klant van de dienst worden verwerkt, is de gevoeligheid van de gegevens hoog.

## Doel

Het doel van deze handreiking is het creëren van inzicht in de juridische dataprotectie aspecten van Smart Mobility-toepassingen waarbij locatiegegevens verzameld en verwerkt worden, bij de doelgroep. Daarnaast beoogt de handreiking een plaats te geven aan data protectie bij het functioneel ontwerp, het technisch ontwerp en de organisatie van Smart Mobility toepassingen, zodanig dat ontwerp- en inrichtingskeuzes expliciet beoordeeld kunnen worden op conformiteit met dataprotectiewetgeving. De toepassing van Privacy by Design zal, naast de bescherming van de privacy van het individu, ook de beveiliging van gegevens ondersteunen ook leiden tot minder data protectie risico's tijdens de operatie, zoals misbruik, onrechtmatig gebruik, vermissing of verminking van persoonsgegevens.

## Doelgroep

De doelgroep voor deze handreiking is primair de dienstverleners. Zij zullen de processen inrichten waarin Privacy by Design ten behoeve van hun klanten wordt ingericht. Daarnaast zijn er secundaire doelgroepen die bij de organisatie van de dienst betrokken kunnen zijn zoals, opdrachtgevers, adviseurs, data-, software-, hardware-leveranciers, klein of groot, ervaren of startup.

## Verantwoordelijke

De verantwoordelijke is degene die doel en middelen voor de verwerking van persoonsgegevens vaststelt en/of die door zijn positie binnen bijvoorbeeld een consortium of in een keten dominant is.
Indien een initiatief of opdracht voor een Smart Mobility project in meer algemene termen is omschreven, is veelal de opdrachtnemer de verantwoordelijke omdat die de eisen van de opdrachtgever of initiatiefnemer vertaalt naar een concreet doel en de bijbehorende middelen.
De overheidsopdracht zal dan ook moeten voorschrijven dat de diensten moeten voldoen aan de principes van Privacy by Design.

## Privacy by Design; 7 ontwerpuitgangspunten

Een erkende manier om tot een goede Privacy by Design aanpak te komen is het framework dat is ontwikkeld door Ann Cavoukian (voormalig Information and Privacy Commissioner van de Canadese provincie Ontario). Het framework kent zeven ontwerpuitgangspunten:

1. Voorkomen is beter dan genezen.
2. Dataprotectie is standaard.
3. Integreren van gegevensbescherming en beveiliging in het ontwerp.
4. Volledige functionaliteit - een positieve balans.
5. Bescherming gedurende de hele levenscyclus.
6. Zichtbaarheid en transparantie.
7. Respect voor de privacy van de gebruiker.

## 1. Voorkomen is beter dan genezen

Dit betekent dat data protectie proactief moet worden opgepakt in de ontwerpfase. Inbreuken op de privacy moeten worden gesignaleerd en verholpen voordat ze zich voordoen; bijvoorbeeld door voorafgaand aan het ontwerpproces een Privacy Impact Analyse (PIA) te doen die de potentiële

privacy risico's in beeld brengt. Kortom, Privacy by Design komt voordat persoonsgegevens worden verwerkt, niet erna!

In Smart Mobility kan aan het volgende gedacht worden bij “voorkomen is beter dan genezen”:

*A verleent een Smart Mobility-dienst in de auto van B. Daarvoor worden gegevens vanuit de auto naar de backoffice gezonden, waaronder het kenteken, dat na de identificatie niet meer van belang is. Het systeem is zo gebouwd dat het kenteken meteen na identificatie en voor de verdere verwerking wordt verwijderd.*

## 2. Dataprotectie is de standaard

Er is maar één manier om zeker te zijn van goede dataprotectie: werken met standaarden. Privacy by Design levert een maximale privacybescherming door ervoor te zorgen dat persoonsgegevens automatisch worden beveiligd ongeacht in welk IT systeem of in welke business-omgeving. In dat geval worden de gegevens standaard beschermd en er is geen actie nodig van de kant van de betrokkene om zijn of haar privacy te beschermen; de bescherming zit standaard in het systeem.

In Smart Mobility kan aan het volgende gedacht worden bij “dataprotectie is de standaard”:

*De gegevens van B, nog steeds persoonsgegevens, worden met zijn toestemming verder door A verwerkt. In het verwerkend systeem is standaard geregeld hoe lang de gegevens bewaard worden, wie toegang heeft tot de gegevens en welke bewerkingen de gegevens op grond van die toestemming mogen ondergaan.*

## 3. Gegevensbescherming en beveiliging integreren in ontwerp

Privacy by Design is ingebakken in het ontwerp van de architectuur van de IT-systemen en in de business-praktijk, en wordt dus niet geleverd als een extra, achteraf. Zo wordt privacy een essentiële component wordt van de basisfunctionaliteit van het systeem, ook als dit betekent dat bepaalde functionaliteit van het systeem daardoor wordt beperkt.

In Smart Mobility kan aan het volgende gedacht worden bij “integreren van gegevensbescherming en beveiliging in het ontwerp”:

*Naast de aard en omvang van de bewerkingen en het voldoen aan de wettelijke voorwaarden zorgt A ervoor dat de gegevens goed zijn beveiligd. Daartoe wordt een toegangsregeling met autorisatie-techniek toegepast, vindt authenticatie plaats en worden berichten zo nodig versleuteld. Ook wordt er bij het opzetten de administratieve organisatie voor gezorgd dat onbevoegden geen toegang kunnen krijgen tot de persoonsgegevens.*

## 4. Volledige functionaliteit, een positieve en geen zero-sum uitkomst

Privacy by Design probeert alle legitieme belangen en doelstellingen te verbinden tot een win-win situatie, in plaats van een zero-sum uitkomst waarbinnen onnodige functionaliteiten en data protectie voorschriften worden geruild. Met Privacy by Design kan worden aangetoond dat het mogelijk is aan zowel data protectie als aan de functionaliteit in het ontwerp recht te doen.

In Smart Mobility kan aan het volgende gedacht worden bij “volledige functionaliteit, een positieve en geen zero-sum uitkomst”:

*De belangen van A en B zijn duidelijk en vooraf ook helder gecommuniceerd. Op grond daarvan heeft B heeft vertrouwen in de dienst van A, in de beveiliging en is hij bereid zijn persoonsgegevens te delen omdat hij erop vertrouwt dat A zich aan de dataprotectie-wetgeving zal houden.*

## 5. End-to-End Security

Een goede beveiligingsstructuur, die is opgezet voordat het eerste gegevenselement is verzameld (verwerkt), legt gedurende de levensduur van de data strenge beveiligingsmaatregelen vast die essentieel zijn voor de bescherming van de privacy, van begin tot eind. Daarmee wordt alle data beveiligd opgeslagen, en vervolgens tijdig en gecontroleerd vernietigd. Zo verzekert Privacy by Design beveiligd informatiemanagement gedurende het hele verwerkingsproces!

In Smart Mobility kan aan het volgende gedacht worden bij “end-to-end security”:

*A zorgt ervoor dat de persoonsgegevens van B niet in onbevoegde handen kunnen vallen. Daartoe neemt hij technische, logistieke en organisatorische maatregelen door de gehele keten. Bovendien wordt het einde van de keten helder gemarkeerd doordat de persoonsgegevens niet langer bewaard dan voor het uitvoeren van de dienst noodzakelijk is.*

## 6. Openheid en transparantie

Privacy by Design is erop gericht om alle stakeholders te verzekeren dat, welke praktijk of technologie ook wordt gebruikt, het systeem opereert volgens de vastgestelde normen en doelen, die op hun beurt weer zijn onderworpen aan onafhankelijke controle. De gebruikte onderdelen en werkwijzen zijn zichtbaar en transparant voor alle stakeholders; credo: vertrouw maar controleer!

In Smart Mobility kan aan het volgende gedacht worden bij “openheid en transparantie”:

*Naast openheid over de belangen geeft A ook vooraf aan hoe hij met persoonsgegevens omgaat in een dataprotectie-verklaring. Daarbij geeft hij inzicht in de wijze waarop de vertrouwelijkheid van de data binnen zijn domein is verzekerd en gaat het om zaken als de getroffen organisatie-maatregelen en bijvoorbeeld encryptie en toegangsbeveiliging.*

## 7. Respect voor de privacy van de gebruiker

Houdt, boven alles, de focus altijd op de eindgebruiker. Privacy is een fundamentele waarde in het leven van de gebruiker. Privacy by Design vraagt van ontwerpers en ontwerpgebruikers om hiermee rekening te houden door maatregelen te nemen als sterke privacy- en basisinstellingen, passende informatieverstrekking, en door gebruiksvriendelijke opties in te bouwen; denk dus gebruiker-georiënteerd!

In Smart Mobility kan aan het volgende gedacht worden bij “respect voor de privacy van de gebruiker”:

*Bij zijn uitingen gaat serviceprovider A uit van de positie van de klant, B. Hij maakt duidelijk hoe hij de wettelijke bepalingen volgt en wat zijn business model is, zodat duidelijk wordt wat hij met de gegevens doet, zoals bijvoorbeeld het wel of niet verkopen van de data.*

## Instrumenten

Om te komen tot goede Privacy by Design is standaardisering nodig en ook toezicht op de toepassing van Privacy by Design. Ook binnen de nieuwe Data Protectie Verordening wordt het accent sterker dan voorheen gelegd op handhaving van de regels, bijvoorbeeld met hogere boetes. De tendens van 'meedelen' naar 'bewijzen' dat de data-protectie goed geregeld is ondersteunt de ontwikkeling van Privacy by Design. In deze paragraaf worden enkele instrumenten genoemd die kunnen helpen bij het inrichten van Privacy by Design.

## Privacy functionaris

De privacy functionaris (PF) wordt op bestuursniveau aangesteld als onafhankelijke beoordelaar van de stand van de data protectie. Hij ziet erop toe dat de data protectie voorschriften worden nageleefd. Dat kan zijn binnen een bedrijf, of binnen een consortium, of zelfs binnen een brancheverenigingen. In de Smart Mobility community zijn alle drie varianten denkbaar. De PF kan door zijn onafhankelijke positie potentiele misstanden aan het licht brengen en het bestuur doen ingrijpen. Daarmee kan overtreding van de data protectie regels in veel gevallen worden voorkomen.

## Privacy Enhancing Technologies

De kern van Privacy by Design bestaat uit Privacy-Enhancing Technologies (PETs): technische maatregelen die gericht zijn op het beschermen van de privacy van betrokkenen, en leiden tot een ‘end-to-end’ beveiliging, identiteits- en toegangsmanagement, en een sterke op de functie gebaseerde authenticatie. De controlemogelijkheden, logging en auditing, van het gegevensverwerkingsproces, maken dat betrokkenen er (blijvend) op kunnen vertrouwen dat hun gegevens niet onrechtmatig worden verzameld, verwerkt, opgeslagen en verspreid. Daarnaast zorgt de verantwoordelijke voor organisatorische maatregelen als functiescheiding en fysieke toegangsbeveiliging.

## Multi-Actor-Analyse

Een Multi-Actor Analyse draagt ertoe bij dat alle actoren en belangen vooraf gedetecteerd worden en de stakeholders zich daarvan bewust zijn. De analyse helpt bij het creëren van voldoende draagvlak bij de stakeholders.

## Privacy Impact Assessment

Een Privacy Impact Analyse (PIA) is een goede methode om de bedreigingen en risico’s in kaart te brengen, die optreden bij de verwerking van

persoonsgegevens. Op grond van de resultaten van de PIA kan bepaald worden welke vormen van Privacy by Design gewenst zijn. Vervolgens moet dit leiden tot een functioneel ontwerp waarin de benodigde functies in hun onderlinge verband worden beschreven.

### Toetsing

Boven alles zal de naleving van de gestelde privacy eisen getoetst moeten worden. Frameworks hiervoor moeten nog worden ontwikkeld. Privacy Patterns (http://privacypatterns.org) kan als een voorbeeld template gekozen worden.

## Bijlage: Nieuwe Wetgeving

### *Nieuwe Verordening Data Protectie (EU) 2016/679*

In de VO PBD opgenomen. de Vo treedt mei 2018 in werking, maar voorsorteren mag, en is zelfs verstandig als de dienst na mei 2018 nog zal bestaan.

#### *Artikel 25* Gegevensbescherming door ontwerp en door standaardinstellingen

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden, treft de verwerkingsverantwoordelijke, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen, zoals pseudonimisering, die zijn opgesteld met als doel de gegevensbeschermingsbeginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen.

2. De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan. Deze maatregelen zorgen met name ervoor dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.

3. Een overeenkomstig artikel 42 goedgekeurd certificeringsmechanisme kan worden gebruikt als element om aan te tonen dat aan de voorschriften van de leden 1 en 2 van dit artikel is voldaan.

#### *Artikel 42* Certificering

1. De lidstaten, de toezichthoudende autoriteiten, het Comité en de Commissie bevorderen, met name op Unieniveau, de invoering van certificeringsmechanismen voor gegevensbescherming en gegevensbeschermingszegels en -merktekens waarmee kan worden aangetoond dat verwerkingsverantwoordelijken en verwerkers bij verwerkingen in overeenstemming met deze verordening handelen. Er

wordt ook rekening gehouden met de specifieke behoeften van kleine, middelgrote en micro-ondernemingen.

2. Ter aanvulling op de naleving door verwerkingsverantwoordelijken of verwerkers die onder deze verordening vallen, kunnen tevens uit hoofde van lid 5 van dit artikel goedgekeurde certificeringsmechanismen voor gegevensbescherming, gegevensbeschermingszegels of -merktekens worden ingevoerd om aan te tonen dat de verwerkingsverantwoordelijken of verwerkers die overeenkomstig artikel 3 niet onder deze verordening vallen, in het kader van de doorgiften van persoonsgegevens aan derde landen of internationale organisaties onder de voorwaarden als bedoeld in artikel 46, lid 2, punt f), passende waarborgen bieden. Die verwerkingsverantwoordelijken of verwerkers doen, via contractuele of andere juridisch bindende instrumenten, bindende en afdwingbare toezeggingen om die passende waarborgen toe te passen, ook wat betreft de rechten van de betrokkenen.
3. De certificering is vrijwillig en toegankelijk via een transparant proces.
4. Een certificering op grond van dit artikel doet niets af aan de verantwoordelijkheid van de verwerkingsverantwoordelijke of de verwerker om deze verordening na te leven en laat de taken en bevoegdheden van de overeenkomstig artikel 55 of 56 bevoegde toezichthoudende autoriteiten onverlet.
5. Een certificaat uit hoofde van dit artikel wordt afgegeven door de in artikel 43 bedoelde certificerende organen of door de bevoegde toezichthoudende autoriteit, op grond van de criteria die zijn goedgekeurd door die bevoegde toezichthoudende autoriteit op grond van artikel 58, lid 3, of door het Comité overeenkomstig artikel 63. Indien de criteria door het Comité zijn goedgekeurd, kan dit leiden tot een gemeenschappelijk certificaat, het Europees gegevensbeschermingszegel.
6. De verwerkingsverantwoordelijke of de verwerker die zijn verwerking aan het certificeringsmechanisme onderwerpt, verstrekt aan het in artikel 43 bedoelde certificeringsorgaan, of, waar van toepassing, aan de bevoegde toezichthoudende autoriteit de voor de uitvoering van de certificeringsprocedure noodzakelijke informatie en verleent het orgaan of de autoriteit toegang tot zijn verwerkingsactiviteiten.
7. Het certificaat wordt afgegeven aan een verwerkingsverantwoordelijke of een verwerker voor een maximumperiode van drie jaar en kan worden verlengd onder dezelfde voorwaarden, mits bij voortduring aan de relevante eisen kan worden voldaan. Indien van toepassing wordt het

certificaat ingetrokken door de in artikel 43 bedoelde certificerende organen of door de bevoegde toezichthoudende autoriteit, wanneer aan de eisen voor de certificering niet of niet meer wordt voldaan.

8. Het Comité verzamelt alle certificeringsmechanismen en gegevensbeschermingszegels en -merktekens in een register en maakt deze via de daartoe geëigende