

## Juridische analyse van het gebruik van IRMA



**Gemeente  
Haarlem**

Auteurs: [REDACTED]  
Datum: 27 februari 2019  
Zaaknummer: 110010068

*Dit advies is opgesteld in opdracht van de Gemeente Haarlem en is opgesteld op basis van de informatie die wij hebben ontvangen van de Gemeente Haarlem. Derden kunnen aan dit rapport geen rechten ontlelen. Op dit rapport zijn de algemene voorwaarden van [REDACTED] van toepassing, te raadplegen via [REDACTED]*

[REDACTED]

## Inhoud

<b>1</b>	<b>INLEIDING EN VRAAGSTELLING</b>	<b>4</b>
<b>2</b>	<b>MANAGEMENTSAMENVATTING</b>	<b>6</b>
<b>3</b>	<b>IRMA EN DE AVG (EN DE WET BRP)</b>	<b>11</b>
<b>4</b>	<b>IRMA EN DE OVERIGE WETGEVING</b>	<b>41</b>

## **1 Inleiding en vraagstelling**

- 1.1.1 De gemeente Haarlem wil gaan experimenteren met de nieuwe authenticatie- en identificatietool 'I Reveal my Attributes' ('IRMA') van de stichting Privacy by Design Foundation (hierna: 'Stichting'). De gemeente is voornemens om via IRMA persoonsgegevens uit de Basisregistratie Personen ('BRP') aan haar burgers beschikbaar te stellen. Deze 'attributen' worden beveiligd opgeslagen in de IRMA-app op de smartphone van de burger. IRMA kan vervolgens op verschillende manieren worden gebruikt.

Allereerst kan IRMA worden gebruikt als authenticatietool. Dit houdt in dat de burger bij transacties of het afnemen van diensten of producten via IRMA specifieke attributen kan tonen aan een derde (de controleur) die noodzakelijk zijn voor het verwezenlijken van de transactie. IRMA kan daarnaast worden gebruikt als identificatietool. De burger kan IRMA gebruiken als identificatiemiddel bij het afnemen van gemeentelijke producten of diensten of producten en diensten van derden. De gemeente Haarlem is voornemens om burgers de mogelijkheid te bieden om zich via de website van de gemeente Haarlem (naast DigiD) ook met IRMA te identificeren.<sup>1</sup>

### **1.2 Vraagstelling**

- 1.2.1 U heeft ons gevraagd om een juridische analyse te verrichten van IRMA. Meer concreet heeft u ons verzocht om te toetsen of zich in het licht van de Algemene Verordening Gegevensbescherming ('AVG') belemmeringen voordoen die zouden maken dat van het IRMA-experiment zou moeten worden afgezien.
- 1.2.2 Daarnaast heeft u ons gevraagd om te toetsen of IRMA voldoet aan de wettelijke regels die gelden voor elektronische identificatiemiddelen, in het bijzonder de eIDAS-verordening en de Wet digitale overheid. Voor wat betreft de eIDAS-verordening heeft u ons verzocht om te na te gaan wat het betrouwbaarheidsniveau is van IRMA (laag, substantieel, midden), voor zover het althans gaat om de specifieke situatie dat de gemeente attributen uitgeeft en controleert.

### **1.3 Scope van dit rapport**

- 1.3.1 Tijdens de bespreking van 22 december 2018 heeft de gemeente aangegeven dat zij geen behoefte heeft aan een uitgebreide toets van alle vereisten van de AVG. De gemeente heeft

<sup>1</sup> IRMA kan tot slot worden gebruikt voor het plaatsen van attribuut-gebaseerde handtekeningen. Een attribuut-gebaseerde handtekening is een speciale digitale handtekening waarbij in de toevoeging aan het document ook een aantal attributen van de ondertekenaar opgenomen worden. Aangezien de gemeente vooralsnog niet voornemens is om van deze functionaliteit gebruik te maken, zal in het verdere vervolg van dit rapport niet nader worden ingegaan op de inzet van IRMA ten behoeve van attribuut-gebaseerde handtekeningen.

ons gevraagd te toetsen of zich op grond van de AVG wezenlijke belemmeringen voordoen die zouden maken dat zou moeten worden afgezien van het IRMA experiment. Wij zullen in dit rapport dan ook enkel stilstaan bij de vereisten van de AVG die (voorafgaand aan de start van het IRMA-experiment) de bijzondere aandacht van de gemeente vereisen.

- 1.3.2 Ten aanzien van de uit de AVG en de eIDAS-verordening voortvloeiende beveiligingsvereisten merken wij op dat dit rapport slechts een juridische toets bevat van de algemene technische beveiliging van IRMA op hoofdlijnen. Daar komt bovendien bij dat de inschatting van het betrouwbaarheidsniveau is beperkt tot de situatie dat IRMA door de gemeente wordt gebruikt voor de uitgifte van credentials. Voor zover de gemeente zekerheid wil verkrijgen over de betrouwbaarheid van de beveiliging dient zij aanvullend een technische audit te verrichten van de beveiliging van IRMA. Dit valt buiten onze expertise.

## **1.4 Opbouw van dit rapport**

- 1.4.1 Dit rapport is als volgt opgebouwd. Hoofdstuk 2 bevat een managementsamenvatting van de belangrijkste bevindingen van dit rapport. In hoofdstuk 3 analyseren wij in hoeverre IRMA voldoet aan de vereisten van de AVG en de Wet BRP. In paragraaf 3.1 zal worden vastgesteld in hoeverre de AVG op IRMA van toepassing is. In paragraaf 3.2 gaan wij in op de verschillende rollen die de gebruikers van IRMA spelen en zal worden vastgesteld wie er optreden als verwerkingsverantwoordelijken en/of verwerker. In paragraaf 3.3 zal worden ingegaan op de vraag of er voor de verwerking van persoonsgegevens een wettelijke grondslag bestaat. Vervolgens zal in paragraaf 3.4 worden besproken of IRMA voldoet aan de materiële vereisten van de AVG. Voor zover de materiële vereisten<sup>2</sup> van de AVG daartoe aanleiding geven, zullen wij toelichten in hoeverre wij belemmeringen zien voor het gebruik van IRMA en/of de gemeente bepaalde acties zal moeten ondernemen om aan de materiële vereisten van de AVG te voldoen. Voor zover belemmeringen worden geconstateerd, zullen wij aanbevelingen doen om ervoor te zorgen dat het IRMA-experiment in overeenstemming met de AVG plaatsvindt.
- 1.4.2 In hoofdstuk 4 van dit rapport toetsen wij het gebruik van IRMA aan de hand van de eIDAS-verordening en het Wetsvoorstel Wet Digitale Overheid. Bij de bespreking van de eIDAS-verordening zullen wij, voor zover mogelijk, een inschatting geven van het betrouwbaarheidsniveau van IRMA.

<sup>2</sup> Het gaat hier kortgezegd om (i) de rechtmatigheid van de verwerking, (ii) de algemene beginselen van de AVG, (iii) de rechten van de betrokkene, (iv) de eisen met betrekking tot de beveiliging. Zie paragraaf 3.4 van dit rapport.

## 2 Managementsamenvatting

- 2.1 In dit rapport zijn wij ten aanzien van het (toekomstig) gebruik van IRMA door de gemeente, voor zover het gaat om de uitgifte en controle van gemeentelijke attributen, tot de volgende conclusies gekomen.

### ***Toepasselijkheid van de AVG***

- Voor zover de gemeente optreedt als *uitgever* van de BRP-attributen aan de gebruiker zal steeds sprake zijn van de verwerking van persoonsgegevens. De door de gemeente uitgegeven BRP-attributen zijn tot de gebruiker herleidbaar. De AVG is van toepassing op de uitgifte van de attributen door de gemeente (randnummers 3.1.1 tot en met 3.1.7).
- Voor zover de gemeente optreedt als controleur is de AVG in verreweg de meeste gevallen van toepassing. Dit is afhankelijk van (i) de aard van de attributen die aan de controleur worden verstrekt en (ii) de aanvullende persoonsgegevens die (al dan niet) automatisch bij het doorlopen van het controleproces worden verwerkt. Voor identificerende attributen zal als uitgangspunt gelden dat de AVG altijd van toepassing is. Is de IRMA-controle beperkt tot niet-identificerende attributen, dan is het mogelijk dat de AVG niet van toepassing is, maar slechts voor zover de gemeente bij het doorlopen van het controleproces geen aanvullende persoonsgegevens (zoals IP-adressen of camerabeelden) verwerkt die – in combinatie met de niet-identificerende attributen – tóch kunnen leiden tot herleidbaarheid tot een natuurlijke persoon (randnummers 3.1.4 tot en met 3.1.13).
- Ook in de relatie tussen de gebruiker en de Stichting zal sprake zijn van het verwerken van persoonsgegevens. Of en zo ja, in hoeverre sprake is van het verwerken van persoonsgegevens is afhankelijk van de vraag of de gebruiker zijn IRMA-account koppelt aan een persoonlijke e-mailadres (randnummer 3.1.14 tot en met 3.1.16).

### ***Verwerkingsverantwoordelijken / verwerkers***

- 2.2 De rollen van de verschillende partijen binnen het IRMA-stelsel kunnen als volgt worden gekwalificeerd:
- de gebruiker van de IRMA-app is de betrokkene;
  - de uitgever (in dit geval de gemeente) handelt als de verwerkingsverantwoordelijke;

- de controleur (in dit geval de gemeente) handelt – voor zover hij althans persoonsgegevens verwerkt van de gebruiker – als verwerkingsverantwoordelijke voor de gegevens die hij opvraagt;
- de Stichting treedt op als verwerkingsverantwoordelijke voor zover het gaat om het verwerken van de persoonsgegevens die de gebruiker tijdens het doorlopen van het registratieproces vrijwillig heeft opgegeven en die de Stichting in het kader van MijnIRMA verwerkt (paragraaf 3.2).

### ***Wettelijke grondslagen voor de verwerkingen***

- De wettelijke grondslag voor de uitgifte van de BRP-gegevens door de gemeente aan de gebruiker zou kunnen worden gevonden in de wettelijke verplichting van de gemeente om – behoudens de wettelijke uitzonderingen die voortvloeien uit de AVG of een bijzondere wet - te voldoen aan een inzageverzoek van de betrokkene (artikel 6, eerste lid, aanhef en onder c, AVG jo. artikel 2:55 Wet BRP jo. artikel 15, eerste lid, AVG). (randnummers 3.3.1 tot en met 3.3.5).
- Ook in de relatie tussen de gemeente als controleur en de gebruiker, bestaat een wettelijke grondslag voor het verwerken van persoonsgegevens door de gemeente. De controle op de identiteit van de betrokkene via IRMA is noodzakelijk om te bewerkstelligen dat de gemeente de gemeentelijke diensten en producten aan de juiste persoon levert (artikel 6, eerste lid, aanhef en onder e, AVG). De wettelijke grondslag 'toestemming' moet zoveel mogelijk door de gemeente worden vermeden, omdat de toestemming naar verwachting niet vrijelijk kan worden gegeven (randnummers 3.3.5 tot en met 3.3.8).
- De gemeente is in haar rol als controleur op grond van artikel 10 Wabb bevoegd tot het verwerken van het burgerservicenummer ('BSN'). (randnummers 3.3.9 tot en met 3.3.12)
- De Stichting is bevoegd tot het verwerken van persoonsgegevens in het kader van MijnIRMA, omdat zij hiervoor toestemming heeft verkregen van de betrokkene (randnummers 3.3.13).

### ***Materiële vereisten van de AVG***

- 2.3 De gemeente heeft ons gevraagd te toetsen of zich op grond van de AVG wezenlijke belemmeringen voordoen die zouden maken dat moet worden afgezien van het IRMA experiment. Wij hebben in dit rapport doen ook enkel stilstaan bij de materiële vereisten die (voorafgaand aan de start van het IRMA-experiment) de bijzondere aandacht van de gemeente vereisen.

2.4 Bij het verrichten van de analyse van IRMA zijn geen wezenlijke belemmeringen geconstateerd voor het van start gaan met het IRMA-experiment. IRMA voldoet in hoofdlijnen aan de materiële voorwaarden van de AVG. Dit neemt niet weg dat er enkele aandachtspunten zijn waarvan de gemeente en de Stichting zich bewust moeten zijn voordat zij van start gaan met het IRMA-experiment. Wij hebben de volgende aandachtspunten bij het gebruik van IRMA door de gemeente geconstateerd en daarbij de volgende aanbevelingen gedaan (hoofdstuk 3.4 van dit rapport).

- ***Geautomatiseerde besluitvorming*** - De gemeente dient er alert op te zijn dat het gebruik van IRMA in specifieke situaties zal kunnen worden aangemerkt als (een onderdeel van) geautomatiseerde individuele besluitvorming. Dit kan in strijd zijn met de AVG en de UAVG (artikelen 22 AVG en artikel 40 UAVG). Het verdient aanbeveling om bij iedere uitbreiding van de inzet van IRMA na te gaan of het gebruik van IRMA mogelijk wordt ingezet ten behoeve van geautomatiseerde besluitvorming en zo ja, of daarvoor een wettelijke grondslag bestaat. Wij raden de gemeente aan om in haar rol als controleur zoveel mogelijk te voorkomen dat IRMA wordt gebruikt ten behoeve van individuele besluitvorming, dan wel het gebruik van IRMA te beperken tot zogenaamde gebonden beschikkingen.
- ***Risico op onjuiste en niet actuele attributen*** - Hoewel de attributen/credentials bij uitgifte worden gewaarmerkt met een digitale handtekening die de controleur bij ontvangst van de attributen van de gebruiker kan controleren, is niet met zekerheid te zeggen of de informatie de persoonsgegevens juist en actueel zijn. De door de gebruiker opgehaalde attributen kunnen inmiddels zijn verouderd. Dit is een inherent risico is aan het gebruik van IRMA. De uitgever (in dit geval de gemeente) kan dit risico enigszins beperken door een geldigheidsdatum te zetten op de door de gebruiker opgehaalde attributen. Het is uiteindelijk de verantwoordelijkheid van de gebruiker om bij wijziging van zijn persoonsgegevens zijn attributen te verversen.
- ***Noodzakelijkheidsbeginsel / dataminimalisatie*** - De gemeente mag in haar rol als controleur bij het gebruik van IRMA niet meer attributen bij de gebruiker mogen opvragen dan strikt noodzakelijk voor het beoogde doel van de IRMA-sessie. Dit betreft een eigen verantwoordelijkheid van de gemeenter, aangezien die zelfstandig bepaalt welke attributen bij de gebruiker worden opgevraagd en welke attributen zij accepteert als voldoende actueel.
- ***Vaststellen bewaartermijn*** - De gemeente moet op grond van artikel 5, eerste lid, aanhef en onder e, AVG een bewaartermijn vaststellen op het verwerken van attributen die zij in haar rol als controleur van de gebruiker verkrijgt. De gemeente dient daarbij als uitgangspunt te nemen dat de bewaartermijn niet langer dan noodzakelijk mag zijn voor de verwerking van de doeleinden waar zij de attributen heeft verkregen en verwerkt.



- **Privacverklaring** - De gemeente zal op grond van artikel 13 AVG de gebruiker voorafgaand aan de verwerking moeten informeren over de verwerking van de persoonsgegevens van de gebruiker. Dit is met name relevant voor zover de gemeente optreedt als controleur. De gemeente zal een op IRMA toegespitste privacyverklaring moeten opstellen.
- **De beveiliging van IRMA** - Voor zover wij kunnen overzien, lijkt IRMA een passend beveiligingsniveau te bieden. IRMA lijkt daarmee te voldoen aan de vereisten van de AVG. Volledige zekerheid kunnen wij echter niet geven. Daarvoor is een uitvoerige technische audit vereist, dat zoals gezegd, buiten onze expertise valt. Enig aandachtspunt is dat IRMA momenteel nog geen back-up mogelijkheid aanbiedt en daardoor mogelijk niet wordt voldaan aan de (beveiligings)voorwaarde dat bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig moet kunnen worden hersteld. In de huidige situatie kan de gebruiker de app slechts blokkeren, opnieuw een account aanmaken en vervolgens wederom alle attributen opvragen bij de uitgevers. Van daadwerkelijk herstellen van de toegang is geen sprake. De Stichting werkt momenteel aan het aanbieden van een back-up mogelijkheid.

### **IRMA en de overige wetgeving**

2.5 Doordat IRMA mede als elektronische identificatiemiddel zal worden gebruikt, dient de gemeente bij het gebruik van IRMA (in aanvulling op de AVG) te voldoen aan de wettelijke regels die gelden voor elektronische identificatiemiddelen. In dit rapport zijn de eIDAS-verordening en het Wetsvoorstel Wet Digitale Overheid belicht.

- De eIDAS-verordening heeft uitsluitend betekenis voor de gemeente zodra een identificatiemiddel met succes is aangemeld bij de Europese Commissie. In een dergelijk geval is de gemeente verplicht om bij het verlenen van haar elektronische diensten het mogelijk te maken dat gebruik kan worden gemaakt van het betreffende identificatiemiddel. Deze verplichting rust in een dergelijk geval echter op alle Europese overheden die elektronische diensten aanbieden. De verwachting is daarom dat op nationaal niveau invulling zal worden gegeven aan de verplichting tot het bieden van de mogelijkheid tot identificatie met een aangemeld elektronisch identificatiemiddel (paragraaf 4.2 van dit rapport).
- De Tweede en de Eerste Kamer hebben nog niet gestemd over het Wetsvoorstel Wet Digitale Overheid. De Wet Digitale Overheid zal mogelijk voorwaarden gaan stellen aan het gebruik van authenticatiediensten zoals IRMA voor het gebruik van digitale overheidsdiensten. Onze verwachting is echter dat dergelijke voorwaarden nog niet op een termijn van twee jaar of korter van kracht zullen worden. Vooralsnog staat de Wet Digitale Overheid dus niet in de weg aan het gebruik van IRMA door de gemeente (paragraaf 4.3 van dit rapport).

***Inschatting betrouwbaarheidsniveau gebruik IRMA door gemeente***

- 2.6 U heeft ons gevraagd om op grond van de eIDAS-verordening een inschatting te geven van het betrouwbaarheidsniveau van het gebruik van IRMA door de gemeente voor zover het gaat om gemeentelijke attributen. Wij merken daarbij op dat wij slechts een inschatting maken van het betrouwbaarheidsniveau van IRMA. Als met zekerheid zou moeten worden vastgesteld wat het betrouwbaarheidsniveau van IRMA is, zou dat een volledige analyse van IRMA en de Stichting vergen. Dat gaat de reikwijdte van dit advies te buiten. Wij zijn, op grond van een algemene toetsing, tot de volgende inschatting gekomen (paragraaf 4.4 van dit rapport).
- De door de gemeente gehanteerde inlogmethode (DigiD met sms) voor de uitgifte van attributen wordt door de eIDAS-verordening aangemerkt met het betrouwbaarheidsniveau 'laag'. Dit straalt af op het totale betrouwbaarheidsniveau van IRMA voor zover het gaat om de uitgifte en controle van gemeentelijke credentials. Doordat het uiteindelijke betrouwbaarheidsniveau van het gebruik van IRMA wordt bepaald door de laagste score, heeft dit automatisch tot gevolg dat het gebruik van IRMA door de gemeente niet hoger kan komen dan betrouwbaarheidsniveau laag.
  - Dit zal anders kunnen komen te liggen in het geval Digid-substantieel of hoog landelijk voor alle burgers beschikbaar wordt. Vanaf dat moment zou het gebruik van IRMA door de gemeente het betrouwbaarheidsniveau 'substantieel' kunnen verkrijgen, mits deze inlogwijze verplicht wordt gesteld door de gemeente en de overige elementen die van belang zijn voor het vaststellen van het betrouwbaarheidsniveau minimaal een betrouwbaarheidsniveau 'substantieel' kunnen garanderen.

### 3 IRMA en de AVG (en de Wet BRP)

#### 3.1 Toepassingsbereik AVG bij IRMA

- 3.1.1 Voordat wordt toegekomen aan de toetsing van IRMA aan de materiële eisen van de AVG, dient allereerst te worden vastgesteld of de AVG van toepassing is. De AVG is van toepassing indien sprake is van de verwerking van persoonsgegevens en de verwerking in een bestand en op een geautomatiseerde wijze plaatsvindt.

Een persoonsgegeven is elk gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon. Van een persoonsgegeven is snel sprake. Het gaat daarbij niet alleen om objectieve informatie (zoals naam, geboortedatum, adres, geslacht en telefoonnummer), maar ook om subjectieve informatie, zoals meningen en oordelen.

Voor de vraag of sprake is van 'identificeerbaarheid' moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is, dan wel door derden, in te zetten zijn om de persoon te identificeren. Daarbij moet rekening worden gehouden met alle objectieve factoren, zoals de kosten van en de tijd benodigd voor identificatie, met inachtneming van de beschikbare technologie op het tijdstip van verwerking en de technologische ontwikkelingen (denk aan de toenemende rekenkracht van computers en het groeiende aantal beschikbare hulpmiddelen).<sup>3</sup>

De AVG is niet van toepassing op gegevens die op zodanige wijze anoniem zijn gemaakt dat de persoon waarop ze betrekking hebben niet meer identificeerbaar is. Iedere mogelijkheid tot identificatie van betrokkene moet onherroepelijk zijn uitgesloten. De Artikel 29-werkgroep<sup>4</sup> heeft in 2014 een opinie over anonimiseringstechnieken gepubliceerd (opinie 5/2014). Daarin worden verschillende anonimiseringstechnieken beschreven. Uit de opinie blijkt onder meer dat het in veel gevallen moeilijk zal zijn om tot volledige anonimiteit te komen:

*"Geen van de in dit advies uiteengezette technieken beantwoordt met zekerheid aan de drie criteria voor een doeltreffende anonimisering, namelijk dat het niet mogelijk mag zijn een persoon te individualiseren (herleidbaarheid), persoonsgebonden records met elkaar in verband te brengen (koppelbaarheid) en persoonsgegevens af te leiden (deduceerbaarheid). Niettemin kan deze of gene techniek sommige van die risico's geheel of ten dele ondervangen. Het is derhalve zaak om zorgvuldig af te wegen hoe een op zichzelf staande techniek kan worden toegepast in de specifieke*

<sup>3</sup> Vgl. Overweging 26 van de AVG.

<sup>4</sup> In deze groep waren de Europese privacytoezichhouders verenigd. De groep bracht onder meer adviezen uit over de interpretatie van begrippen in de privacyrichtlijn. De groep was zeer gezaghebbend. Sinds de inwerkingtreding van de AVG heeft de European data protection board ('EDPB') de taken van de Artikel-29 Werkgroep overgenomen. De EDPB heeft de eerdere adviezen van de artikel-29 Werkgroep bekrachtigd.

*situatie die aan de orde is. Voorts moet worden bekeken of een combinatie van die technieken ertoe kan bijdragen het resultaat beter bestand te maken tegen privacyschendingen.” (p. 27).*

3.1.2 In het licht van het voorgaande zal eerst moeten worden vastgesteld of er persoonsgegevens worden verwerkt bij het gebruik van IRMA als authenticatiemiddel. Het antwoord op deze vraag kan verschillen per relatie die tot stand komt bij het gebruik van IRMA. Er vallen grofweg drie relaties te onderscheiden, te weten:

- (a) De relatie tussen de gebruiker en de uitgever;
- (b) De relatie tussen de gebruiker en de controleur;
- (c) De relatie tussen de gebruiker en de Stichting.

3.1.3 Hierna zullen we per relatie vaststellen of en zo ja, in hoeverre er binnen de afzonderlijke relaties sprake is van de verwerking van persoonsgegevens.

***Ad (a) De gebruiker en de uitgever***

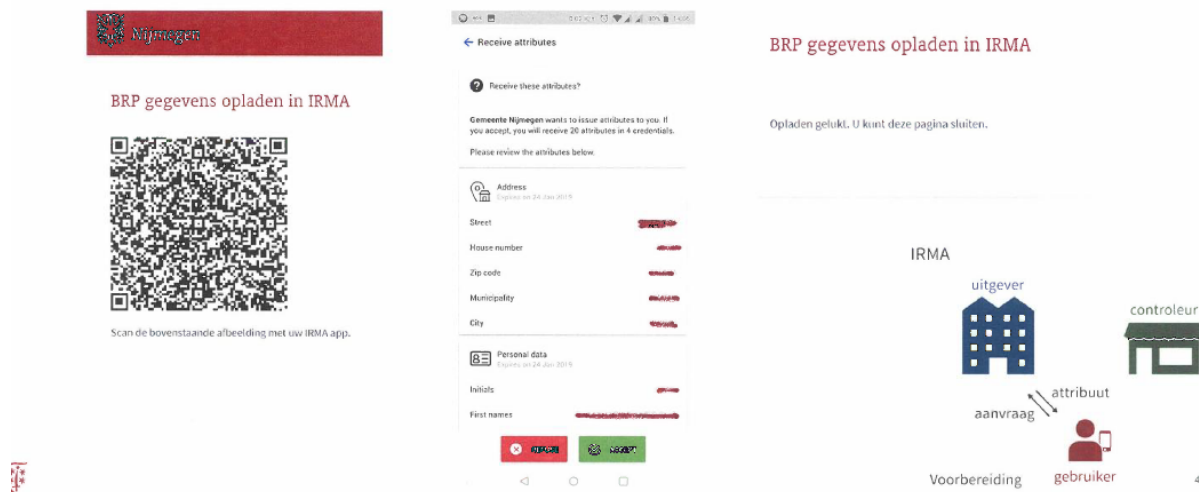
3.1.4 Het ophalen van de attributen gaat als volgt. De burger logt met DigiD in op de website van de gemeente Haarlem (**stap 1**). Op de website van de gemeente Haarlem wordt een QR-code getoond die de burger met zijn smartphone kan scannen. De burger ontgrendelt zijn IRMA-app door eerst zijn persoonlijke PIN in te voeren.<sup>5</sup> Nadat de burger de QR-code met zijn IRMA-app heeft gescand, verschijnt er op het scherm van de smartphone van de burger een toestemmingsformulier voor het ophalen van de BRP-gegevens van de burger (**stap 2**).<sup>6</sup> Geeft de burger zijn expliciete toestemming, dan worden de gegevens (automatisch) door de gemeente verstrekt en ingeladen op de IRMA-app van de gebruiker.

<sup>5</sup> Het invoeren van de PIN voorafgaand aan het verkrijgen van de toegang tot de IRMA-app betreft een recentelijk door de Stichting ingevoerde beveiligingsmaatregel. Ten tijde van het schrijven van dit rapport was deze beveiligingsmaatregel nog slechts gereleased voor Android telefoons. Wij gaan er vanuit dat bij het uitbrengen van dit rapport de verplichte invoer van de PIN om toegang te verkrijgen tot de IRMA-app voor alle versies van de IRMA-app - en aldus ook voor de iPhone - zal gelden.

<sup>6</sup> Zoals wij hierna achter randnummer 3.4.15 van dit rapport zullen toelichten, ziet de Stichting weliswaar dat een QR-code is gescand en dat de uitgifte van attributen heeft plaatsgevonden, maar kan de Stichting niet zien welke persoonsgegevens zijn uitgegeven.

## Overhalen van gegevens in IRMA

- Burger scant de QR met IRMA app en geeft goedkeuring voor het overhalen van de attributen



3.1.5 De uitgifte van de BRP-gegevens door de gemeente omvat de volgende attributen:

Adres	Persoonsgegevens	Leeftijdcontroles	BSN
Straat	Intialen	Over 12	BSN
Huisnummer	Voornaam	Over 16	
Postcode	Achternaam	Over 18	
Gemeente	Geboortedatum	Over 21	
Stad	Geslacht	Over 65	
	Nationaliteit		

3.1.6 De attributen worden gezamenlijk aangeduid als 'credentials'. De attributen worden door de gemeente voorzien van een digitale handtekening. Bij het latere gebruik van de attributen door de gebruiker kan de controleur aan de hand van de digitale handtekening de authenticiteit van de attributen controleren.<sup>7</sup> Nadat de digitale handtekening is geplaatst en de attributen/credentials aan de gebruiker zijn verstrekt, kan de uitgever (in dit geval de gemeente), voor zover het gaat om attributen die niet-identificerend zijn en de uitgever zou samenwerken met controleurs, het latere gebruik van de attributen door de gebruiker niet meer kunnen traceren.<sup>8</sup>

### Toepasselijkheid AVG

<sup>7</sup> Zie hierover randnummer 3.5.15 van dit rapport.

<sup>8</sup> Dit wordt aangeduid als 'issuer unlinkability'.

- 3.1.7 In de relatie tussen de gebruiker en de uitgever (in dit geval de gemeente) is, naar wij menen, steeds sprake van het verwerken van persoonsgegevens. De hiervoor beschreven attributen zijn naar hun aard zowel afzonderlijk als gezamenlijk persoonsgegevens van de gebruiker. Van de verwerking van persoonsgegevens is hoe dan ook sprake, reeds alleen al, omdat de attributen direct herleidbaar zijn tot de verzoekende gebruiker en de gemeente (in)direct op de hoogte is van de identiteit van de verzoeker. De verstrekking van de BRP-gegevens door de gemeente is aldus een verwerking in de zin van de AVG. De gemeente verwerkt bovendien bij het doorlopen van het uitgifteproces naar alle waarschijnlijkheid ook andersoortige persoonsgegevens van de gebruiker. De gemeente verwerkt naar verwachting (aanvullend) via haar website de DigiD en het IP-adres van de burger. Het voorgaande leidt tot de slotsom dat de AVG bij de uitgifte van de attributen altijd van toepassing is.<sup>9</sup>

***Ad (b) De gebruiker en de controleur***

- 3.1.8 De gebruiker kan zijn opgehaalde attributen in de IRMA-app gebruiken om op verzoek van een derde (de zogenaamde 'controleur' en dit geval de gemeente) ter authenticatie of identificatie aan de gemeente te tonen. De gebruiker kan de verschillende attributen los van elkaar, maar ook in verschillende combinaties tonen.<sup>10</sup> Dit gaat als volgt.
- 3.1.9 De gebruiker wil via de website van de gemeente een product of dienst afnemen. De gemeente treedt in dit geval op als controleur. De gemeente biedt via haar website de gebruiker de mogelijkheid aan om - naast DigiD - ook met IRMA te identificeren. De gebruiker verkrijgt toegang tot zijn IRMA-app door middel van het invoeren van zijn geheime PIN. Indien de gebruiker door middel van IRMA wil inloggen, scant de gebruiker de QR-code op de website van de gemeente. Op het scherm van de smartphone van de gebruiker verschijnt een toestemmingsformulier waarin de IRMA-app vraagt om expliciete toestemming voor het verstrekken van attributen (in dit geval het BSN) aan de gemeente. De gebruiker geeft zijn expliciete toestemming door op akkoord te drukken. Het attribuut wordt vervolgens aan de gemeente verstrekt.

<sup>9</sup> Bij deze analyse is als uitgangspunt genomen dat de gemeente Haarlem ervoor kiest om zelfstandig via haar eigen server over te gaan tot de uitgifte van attributen. Het is echter technisch mogelijk dat de gemeente bij de uitgifte van attributen gebruikmaakt van de diensten van een derde of de Stichting. In deze situaties verwerken derden namens de gemeente persoonsgegevens van de gebruiker. Wij raden dit in beginsel af, omdat de persoonsgegevens in dat geval (onnodig) met anderen worden gedeeld. Daarbij geldt bovendien dat de door de gemeente ingeschakelde derden, naar verwachting, zullen optreden als verwerker. De AVG verplicht de gemeente in een dergelijk geval tot het afsluiten van de (verwerkers)overeenkomst met de door haar ingeschakelde partij.

<sup>10</sup> Dit wordt aangeduid als 'selective disclosure'.

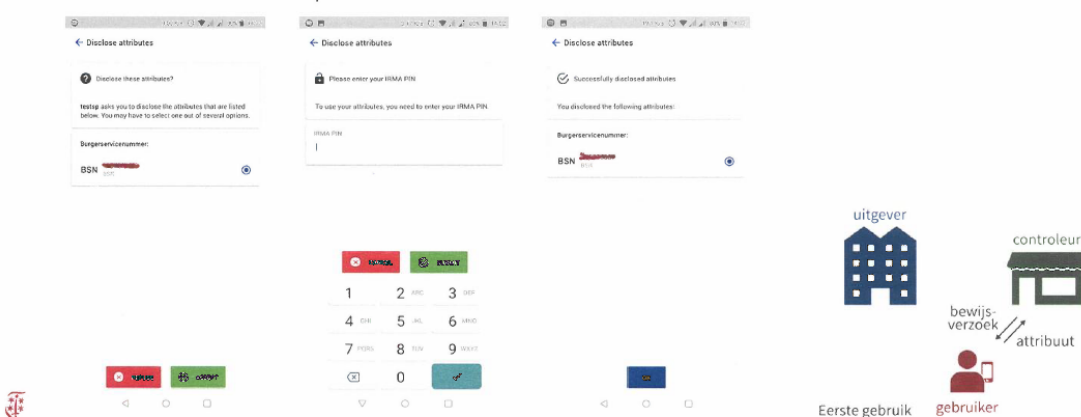
## Controle van Gegevens

- De burger vraagt een product of dienst aan via de website en kan zich naast Digidig ook met IRMA identificeren



## Akkoord van burger en delen gegevens

- Gebruiker geeft toestemming voor delen van zijn attribuut, BSN
- Vult ter controle de pincode in



3.1.10 Bij het verkrijgen van de attributen via IRMA controleert de controleur (in dit geval de gemeente) de verkregen attributen (geautomatiseerd) op de volgende aspecten:

- zijn de attributen nog geldig (niet verlopen);
- klopt de digitale handtekening op de credentials en daarmee de authenticiteit van de attributen;
- zijn de attributen/credentials afkomstig van een uitgever die de controleur voldoende vertrouwt voor deze transactie;
- behoren de attributen uit meerdere credentials tot dezelfde persoon?

- 3.1.11 Indien akkoord, verkrijgt de gebruiker toegang tot het beveiligde deel van de website van de controleur en kan hij de transactie en/of de aanvraag van de producten of diensten afronden.<sup>11</sup>

*Toepasselijkheid AVG*

- 3.1.12 In de relatie tussen de gebruiker en de controleur is niet op voorhand duidelijk of in alle gevallen persoonsgegevens worden verwerkt. Dit is, evenals het geval is bij de uitgifte van attributen, in belangrijke mate afhankelijk van de volgende omstandigheden:

- *de aard van de attributen die aan de controleur worden verstrekt*

Van een verwerking van persoonsgegevens is pas sprake indien de getoonde attributen afzonderlijk, dan wel gezamenlijk (in)direct herleidbaar zijn tot de gebruiker. Dit is geheel afhankelijk van de inhoud van de IRMA-uitvraag. Is de uitvraag beperkt tot niet-identificerende attributen (bijv. de vraag of iemand 18+ is), dan is verdedigbaar dat het tonen van dat attribuut en het raadplegen daarvan door de controleur op zichzelf niet tot het verwerken van persoonsgegevens. De AVG is mogelijk niet van toepassing, mits wordt gewaarborgd dat geen aanvullende persoonsgegevens worden verwerkt die alsnog kunnen leiden tot identificatie van de gebruiker (zie volgende bullet). Dit ligt uiteraard anders indien de uitvraag ziet op identificerende attributen zoals het BSN en/of iemands adres. In een dergelijk geval zijn de attributen altijd herleidbaar tot de gebruiker en zal er aldus sprake zijn van het verwerken van persoonsgegevens. De AVG is in dat geval van toepassing. De gemeente verwerkt de door haar opgehaalde attributen voor zo lang als zij, na voltooiing van het controleproces, de opgehaalde gegevens in haar systemen bewaart.<sup>12</sup>

- *de (eventuele) aanvullende persoonsgegevens die automatisch worden verwerkt door de controleur (onder meer IP-adres)*

Zelfs indien de IRMA-uitvraag is beperkt tot attributen die op zichzelf niet direct herleidbaar zijn tot de gebruiker, dan nog is het mogelijk dat de AVG van toepassing is. Dit heeft te maken met de eventuele aanvullende (persoons)gegevens die (automatisch) door de controleur worden verwerkt

<sup>11</sup> Evenals bij de uitgifte van attributen/credentials is het technisch mogelijk dat de controleur derden inschakelt bij het uitvoeren van (een deel van) de controle op de authenticiteit van de verkregen attributen. Zoals reeds toegelicht achter voetnoot 9 van dit rapport, zal de gemeente Haarlem de controle en uitgifte zelfstandig uitvoeren.

<sup>12</sup> Aanbeveling daarbij is dat de gemeente, voor zover zich geen wettelijke bewaartermijn voordoet, de gegevens te verwijderen op het moment dat de gegevens niet meer noodzakelijk zijn voor de door de gemeente nagestreefde doeleinden.



bij het doorlopen van de IRMA-authenticatieprocedure. Wij lichten dit toe met een voorbeeld.

Het is goed denkbaar dat de controleur (bijv. de gemeente) bij het doorlopen van de IRMA-authenticatieprocedure via zijn website het IP-adres van (de computer of de telefoon van de) gebruiker verwerkt. Aangezien een IP-adres een zelfstandig persoonsgegeven is over de gebruiker<sup>13</sup>, is het mogelijk dat de controleur bij het verwerken daarvan gebonden is aan de regels van de AVG. De verwerking van het IP-adres heeft ook een ander gevolg. De koppeling van het IP-adres met de attributen kan ertoe leiden dat de niet-identificerende attributen die eerst geen persoonsgegevens waren, tóch persoonsgegevens worden. Het niet-identificerende attribuut *in combinatie met* het IP-adres kan er namelijk toe leiden dat het attribuut wel degelijk (in)direct herleidbaarheid is tot de betrokkene. Het attribuut kwalificeert daardoor alsnog als een persoonsgegeven.

Bovengenoemd voorbeeld ziet op het aanvullend verwerken van het IP-adres. Het risico op herleidbaarheid kan uiteraard ook ontstaan bij het (aanvullend) verwerken van andere persoonsgegevens. Gedacht kan worden aan de fingerprint van de browser, camerabeelden van de betrokkene en/of gezichtsherkenning.

Een en ander maakt dat ook in de situatie dat de gebruiker via IRMA op eerste oogopslag anonieme, niet-identificerende attributen aan de controleur toont, sprake kan zijn van een verwerking van persoonsgegevens waarop de AVG van toepassing is.<sup>14</sup>

- 3.1.13 Aangezien naar verwachting in verreweg de meeste gevallen sprake zal zijn van het verwerken van persoonsgegevens, verdient het aanbeveling om er steeds van uit te gaan dat de AVG van toepassing is op de gegevensstroom die plaatsvindt tussen de gebruiker en de gemeente in haar rol als controleur.<sup>15</sup>

<sup>13</sup> Uitgangspunt is dat een IP-adres een persoonsgegeven vormt over de betrokkene.

<sup>14</sup> Hoewel het gebruik van IRMA niet maakt dat de AVG niet langer van toepassing is, beperkt IRMA de verwerking van persoonsgegevens tot het strikt noodzakelijke. Dit is in lijn met het dataminimalisatie-beginsel en de beginselen van privacy by design & default. De cryptografische versleuteling en de splitsing van de private en public key fungeert voorts als een beveiligingsmaatregel.

<sup>15</sup> Voor alle duidelijkheid: het is denkbaar dat de AVG in specifieke situaties niet van toepassing is. Deze situatie doet zich voor in het geval de IRMA-uitvraag (i) is beperkt tot niet-identificerende attributen en (ii) de controleur en/of de gebruiker (technische) maatregelen treffen die bewerkstelligen dat geen aanvullende persoonsgegevens worden verwerkt. Het is op dit moment niet duidelijk of en zo ja, hoe vaak authenticatie geheel anoniem zal plaatsvinden. Bovendien is het nog maar de vraag of het technisch haalbaar is dat aanvullende persoonsgegevens niet worden verwerkt. Bij twijfel raden wij in ieder geval aan om ervan uit te gaan dat sprake is van het geautomatiseerd verwerken van persoonsgegevens waarop de AVG van toepassing is.

### **Ad (c) De gebruiker en de Stichting**

- 3.1.14 Ook in de relatie tussen de gebruiker en de Stichting zal in veel gevallen sprake zijn van het verwerken van persoonsgegevens. De Stichting heeft weliswaar geen beschikking over de IRMA attributen op de telefoon van de gebruiker, maar verwerkt wel een beperkt aantal andere persoonsgegevens die de Stichting tijdens het registratieproces van de gebruiker heeft verkregen.

De Stichting vervult in het huidige IRMA-stelsel verschillende rollen. Allereerst speelt zij een rol bij de controle van de invoering van de juiste PIN en de uitvoer van het sleutelbeheer, zodat uitgifte en controle van attributen kan plaatsvinden. Daarnaast vervult de Stichting de rol van (verwerkings)verantwoordelijke van de 'MijnIRMA-website'. De gebruiker heeft via de MijnIRMA-website de mogelijkheid om inzage te verkrijgen in de gebruiksgegevens en – voor zover dit noodzakelijk is (bijv. in het geval van diefstal) – het gebruik van de IRMA-app te blokkeren. Het is niet uitgesloten dat de rol van de Stichting bij toekomstig gebruik zal gaan veranderen. Het is bij verdere doorontwikkeling en adoptie van IRMA mogelijk dat de huidige rollen van de Stichting zullen worden gedecentraliseerd en zullen overgenomen door de controleurs of uitgevers zelf, dan wel andere daartoe aangewezen derden.

- 3.1.15 In hoeverre persoonsgegevens van de gebruiker door de Stichting worden verwerkt, is in belangrijke mate afhankelijk van de keuzes die de gebruiker bij het registratieproces heeft gemaakt. Twee opties zijn denkbaar:

- *de gebruiker kiest tijdens het registratieproces een PIN code en ziet af van het opgeven van zijn e-mailadres<sup>16</sup>*

In dit geval verwerkt de Stichting slechts de willekeurige gebruikersnaam die automatisch door IRMA voor de gebruiker wordt gegenereerd na het voltooien van het registratieproces. In aanvulling hierop verwerkt de Stichting per gebruiker de loggegevens van het gebruik van de IRMA-app. De loggegevens geven enkel inzicht in wanneer de gebruiker attributen heeft getoond en wanneer de IRMA-app attributen heeft ontvangen. Uit de loggegevens kan niet worden opgemaakt om welke attributen het gaat, aan welke controleur de attributen zijn getoond of van welke uitgever de gebruiker attributen heeft ontvangen. Wel geven de loggegevens inzicht in de aard van de acties, zoals 'PIN geverifieerd' of 'IRMA sessie uitgevoerd'. Het doel van het verwerken van de loggegevens is dat de Stichting of de gebruiker zelf (via MijnIRMA) misbruik kunnen detecteren, bijvoorbeeld in het geval een IRMA-account buitensporig veel wordt gebruikt (hetgeen kan

<sup>16</sup> Het opgeven van een e-mailadres bij de registratie is niet verplicht.

duiden op misbruik). De Stichting of de gebruiker kunnen via MijnIRMA in een dergelijk geval overgaan tot het blokkeren van het IRMA-account met als gevolg dat de gebruiker zijn attributen niet meer kan gebruiken.

Wij menen dat de automatisch gegenereerde gebruikersnaam en de loggegevens geen persoonsgegevens betreffen, tenzij de gebruikersnaam in combinatie met andere aanvullende gegevens (indirect) herleidbaar zou zijn tot de gebruiker. Naar wij begrijpen is dat voor de Stichting niet mogelijk, omdat zij haar systeem zo heeft ingesteld dat geen contactgegevens van de smartphones van gebruikers (zoals bijv. het IP-adres) worden verwerkt. We achten het in dit licht verdedigbaar dat de Stichting, in de huidige situatie, inderdaad geen persoonsgegevens van een gebruiker verwerkt, indien het IRMA-account niet is gekoppeld aan een persoonlijk e-mailadres.<sup>17</sup>

- *de gebruiker kiest een PIN code en koppelt zijn IRMA-account aan zijn e-mail*

De gebruiker heeft ook de mogelijkheid om zijn IRMA-account te koppelen aan zijn e-mailadres. Vanzelfsprekend zal in dat geval de gebruikersnaam en de loggegevens eerder herleidbaar zijn tot de gebruiker. Hierdoor zal sprake zijn van het verwerken van persoonsgegevens. De AVG is in dit geval van toepassing.

- 3.1.16 Het voorgaande leidt tot de slotsom dat de Stichting in specifieke gevallen continue persoonsgegevens verwerkt, in ieder geval voor zover de gebruiker zijn IRMA-account heeft gekoppeld aan zijn persoonlijke e-mailadres. Dit maakt dat de AVG van toepassing is.
- 3.1.17 De Stichting verwerkt ook in specifieke individuele situaties de persoonsgegevens van de gebruiker. De Stichting verkrijgt bij een eventuele crash van de IRMA-app een rapport over de fout die is opgetreden. Dit rapport bevat onder meer het IP-adres, hetgeen een persoonsgegeven betreft over de gebruiker. Dit maakt dat in ook in die situatie sprake is van een verwerking van persoonsgegevens waarop de AVG van toepassing is.<sup>18</sup>

<sup>17</sup> Dit gaat uiteraard alleen op voor zover de Stichting niet op een andere wijze de beschikking verkrijgt over persoonsgegevens van de betrokkene.

<sup>18</sup> Hoewel zich deze situatie in het geval van gemeente Haarlem niet voordoet, is het mogelijk dat de Stichting wordt ingeschakeld om namens de uitgever attributen uitgeeft. Wij merken ten overvloede op dat de Stichting in dat geval naar verwachting optreedt als verwerker voor de uitgever. De Stichting zou aldus ook in die situatie gebonden zijn aan de voorwaarden van de AVG.

### ***Toekomstige ontwikkeling: Het beheren van backups***

*Tijdens de bespreking van 22 december jl. met de gemeente en de Stichting kwam aan bod dat de Stichting voornemens is om aan gebruikers de functionaliteit aan te bieden om een back-up van de attributen in de IRMA-app te maken. De back-up wordt beveiligd, gespeudonimiseerd en kan – bij eventueel verlies of diefstal – opnieuw door de gebruiker op zijn IRMA-app worden gezet. Vooralsnog is niet duidelijk wie het beheer van de back-ups op zich zal nemen en welke rol de Stichting bij het beheren van de back-ups zal spelen.*

*Aandachtspunt bij het kiezen de locatie van de back-up, is dat het beheren van de back-up een zelfstandige verwerking van persoonsgegevens vormt. De back-up bevat immers attributen die herleidbaar zijn tot de gebruiker. Het verwerken van de back-ups en de daarin opgenomen persoonsgegevens is slechts toegestaan voor zover daarvoor een wettelijke grondslag bestaat en aan de overige vereisten van de AVG wordt voldaan.<sup>19</sup> Daarbij is niet relevant of inzage wordt verkregen in de attributen die zijn opgenomen in de backups. Doordat het BSN onderdeel uitmaakt van de attributen, zal naar alle waarschijnlijkheid een derde niet snel bevoegd zijn om de back-up te verwerken. Dit zou aanleiding kunnen vormen om te beslissen dat de gebruiker zelf zijn back-up beheert.*

## **3.2 Hoe kwalificeren de verschillende rollen?**

- 3.2.1 Nu uit de voorgaande paragraaf volgt dat de AVG in ieder geval op een deel van de gegevensstromen van toepassing is, rijst de vraag hoe de verschillende actoren kwalificeren in de zin van de AVG. De AVG maakt onderscheid tussen de volgende rollen:

De verwerkingsverantwoordelijke is degene die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.<sup>20</sup> Omdat de verwerkingsverantwoordelijke degene is die het doel van en de middelen voor de gegevensverwerking vaststelt, rusten veel van de verplichtingen van het gegevensbeschermingsrecht op de verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke is bevoegd tot het verwerken van persoonsgegevens indien daarvoor een wettelijke grondslag bestaat.

De verwerker is degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.<sup>21</sup> De verwerker ontleent zijn bevoegdheid om

<sup>19</sup> Voor zover wij kunnen overzien, lijkt enkel de toestemming van de gebruiker van IRMA een wettelijke grondslag in de zin van artikel 6, eerste lid, AVG op te leveren voor het verwerken van de back-up. Het is evenwel de vraag of de enkele toestemming voldoende is indien ook het BSN onderdeel uitmaakt van de back-up. De derde bij wie de back-up zal worden opgeslagen zal in beginsel niet bevoegd zijn tot het verwerken van het BSN, althans niet voor dit doel.

<sup>20</sup> Artikel 4 aanhef en onder 7, AVG.

<sup>21</sup> Artikel 4, aanhef en onder 8, AVG.

persoonsgegevens te verwerken aan de bevoegdheid van de verwerkingsverantwoordelijke die hem inschakelt. De bevoegdheden van een verwerker moeten zijn vastgelegd in een verwerkersovereenkomst.<sup>22</sup>

De verwerker kan met voorafgaande toestemming van de verwerkingsverantwoordelijke een subverwerker inschakelen. De bevoegdheden van de subverwerker moeten eveneens zijn vastgelegd in een (sub)verwerkersovereenkomst.

3.2.2 De beantwoording van de vraag wie binnen het IRMA-stelsel kan worden aangemerkt als betrokkene, verwerkingsverantwoordelijke of verwerker is relevant om hierna per actor te kunnen bepalen welke eisen uit de AVG van toepassing zijn en op welke wijze aan die eisen uitvoering moet worden gegeven. Wij komen tot de volgende conclusies:

- **de gebruiker van de IRMA-app is de betrokkene**
- **de uitgever (in dit geval de gemeente) handelt als de verwerkingsverantwoordelijke**

De uitgever beschikt over de authentieke attributen en beslist zelfstandig of hij gebruik wil maken van IRMA. Bovendien bepaalt de uitgever welke attributen aan de gebruiker worden vrijgegeven. De uitgever bepaalt daarmee het doel en de middelen van de verwerking.

- **de controleur handelt – voor zover hij althans persoonsgegevens verwerkt van de gebruiker<sup>23</sup> – als verwerkingsverantwoordelijke.**

De controleur bepaalt dat hij gebruik wil maken van IRMA en bepaalt daarnaast welke attributen hij van de gebruiker wenst te ontvangen. Voor zover bij de controle van de attributen persoonsgegevens zijn gemoeid, bepaalt de controleur het doel en de middelen van de verwerking en treedt hij aldus op als verwerkingsverantwoordelijke.

- **de Stichting treedt op als verwerkingsverantwoordelijke**

De Stichting treedt op als verwerkingsverantwoordelijke voor zover het gaat om het verwerken van de persoonsgegevens die de gebruiker tijdens het doorlopen van het registratieproces vrijwillig heeft opgegeven en die de Stichting in het kader van MijnIRMA verwerkt. De verwerking is zeer

<sup>22</sup> Artikel 28, derde lid, AVG.

<sup>23</sup> Zie voorgaande paragraaf waarin wij hebben besproken in welke situaties bij het gebruik van IRMA sprake is van de verwerking van persoonsgegevens.



beperkt: het gaat hier met name om het e-mailadres van de gebruiker. Bepalend is of de gebruiker tijdens het registratieproces zijn IRMA-account heeft gekoppeld aan zijn persoonlijke e-mailadres.<sup>24</sup> Is dit het geval dan zullen ook de loggegevens herleidbaar zijn tot de gebruiker. Doordat de verwerking beperkt is, zal een eenvoudige verwerkersovereenkomst volstaan.

### **3.3 Wettelijke grondslag voor de verwerkingen**

3.3.1 Het verwerken van persoonsgegevens kan slechts rechtmatig plaatsvinden indien de verwerking kan worden gebaseerd op een wettelijke grondslag. Dit kan een wettelijke grondslag zijn die volgt uit de algemene wettelijke grondslagen van de AVG of een specifieke wettelijke grondslag die volgt uit een bijzondere wet. De algemene wettelijke grondslagen zijn opgenomen in artikel 6 AVG.

Vgl. Artikel 6, eerste lid, AVG:

De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan:

- a) de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
- b) de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
- c) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
- d) de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
- e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
- f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

<sup>24</sup> Voor een nadere toelichting verwijzen wij naar randnummers 2.1.15 e.v. van dit rapport.

- 3.3.2 In de hierna volgende paragrafen zullen wij per gegevensstroom tussen de gebruiker, uitgever, de betrokkene en de Stichting analyseren of een wettelijke grondslag aanwezig is voor de verwerking van persoonsgegevens.

#### **Ad (a) De gebruiker en de uitgever**

##### *Wettelijke grondslag AVG*

- 3.3.3 De gebruiker neemt bij IRMA het initiatief om zijn attributen bij de uitgever (in dit geval de gemeente) op te vragen. De vraag rijst hoe de uitvraag van de attributen door de gebruiker kan worden gekwalificeerd. In feite verzoekt de gebruiker om een kopie van zijn persoonsgegevens. Het op verzoek verstrekken van de attributen aan de gebruiker kan worden gezien als een (beperkte) uitvoering van het recht op inzage door de uitgever (de gemeente).<sup>25</sup> De verstrekking van de BRP-gegevens aan de gebruiker ter uitvoering van het inzageverzoek kan vervolgens worden gevonden in de wettelijke plicht van de gemeente in de zin van artikel 6, eerste lid, aanhef en onder e, AVG om – behoudens eventuele weigeringsgronden – aan een verzoek op grond van artikel 15, eerste lid, AVG te voldoen.

##### *Wettelijke grondslag Wet BRP*

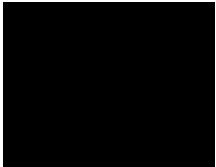
- 3.3.4 Voor zover de gemeente optreedt als uitgever, doet zich de bijzondere situatie voor dat er persoonsgegevens worden verstrekt uit de BRP. Dit gegeven maakt dat niet slechts de AVG, maar ook de Wet BRP van toepassing is op de verstrekking van de attributen door de gemeente.<sup>26</sup> Het ophalen van de attributen bij de gemeente kwalificeert in feite als een inzageverzoek van de burger in zijn BRP-gegevens. De burger verkrijgt immers een deel van de persoonsgegevens die zijn opgenomen in de persoonslijst. Een dergelijk inzageverzoek wordt zowel gereguleerd door (de algemene regels van) de AVG als (de meer specifieke regels van) de Wet BRP.<sup>27</sup>

De Wet BRP biedt in onze optiek voldoende ruimte voor het door de gemeente verstrekken van attributen uit de BRP aan de gebruiker via IRMA. Feitelijk brengt het

<sup>25</sup> Wij spreken hier van een 'beperkte uitvoering' van het recht op inzage, omdat artikel 15 AVG diverse voorwaarden stelt aan de informatie die op verzoek van de betrokkene moet worden verstrekt. Naast een overzicht van de persoonsgegevens, dient bijvoorbeeld informatie te worden gegeven over de ontvangers van de persoonsgegevens, internationale doorgifte, gehanteerde bewaartermijnen en de verwerkingsdoeleinden. Hoewel de uitvraag van de attributen aldus *lijkt* op een verzoek om inzage ex artikel 15 AVG, is het dat strikt genomen niet. In het geval van een uitvraag van attributen verkrijgt de gebruiker van IRMA namelijk enkel een kopie van zijn persoonsgegevens, zonder de in artikel 15 AVG opgenomen aanvullende informatie.

<sup>26</sup> Voorheen was het zo dat de voorloper van de AVG – de Wet bescherming persoonsgegevens ('Wbp') – niet van toepassing was op de verwerking van persoonsgegevens die is geregeld bij of krachtens de Brp (artikel 2 lid 2 aanhef en onder d Wbp). Onder de AVG is dat anders. Op de verwerking van persoonsgegevens voor zover daarop de Wet Brp van toepassing is, zal de Uitvoeringswet AVG niet van toepassing zijn (artikel 2 lid 2 wetsvoorstel Uitvoeringswet AVG), maar de AVG wel. Uit de memorie van toelichting bij het wetsvoorstel Uitvoeringswet AVG blijkt dat in de Wet Brp zelfstandig uitvoering aan de AVG zal worden gegeven. Zie *Kamerstukken II* 2017/18, 34 851, nr. 3, p. 79.

<sup>27</sup> Artikel 15, eerste lid, AVG jo. artikel 2.55, eerste lid, BRP.



experiment van IRMA enkel veranderingen teweeg in de wijze waarop de BRP-gegevens door de gemeente aan de burger worden verstrekt. Dit is in lijn met de Wet BRP, nu de wijze van het verstrekken van BRP-gegevens slechts beperkt wordt gereguleerd door de Wet BRP. Wij lichten dat hieronder nader toe.

Een betrokkene heeft op grond van de Wet BRP het recht om inzage te krijgen in zijn BRP-gegevens (artikel 2.55 Wet BRP). De betrokkene kan zijn verzoek richten tot zijn eigen gemeente, dan wel ieder ander willekeurige gemeente.<sup>28</sup> Voor zover zich geen weigeringsgronden voordoen, verstrekt de gemeente aan de betrokkene een volledig overzicht van de persoonslijst van de betrokkene.<sup>29</sup> De Wet BRP stelt geen - althans zeer beperkte - voorwaarden aan de wijze waarop een verzoek mag worden ingediend en de wijze waarop de gemeente daaraan uitvoering geeft. De Wet BRP stelt slechts dat (i) het college de identiteit van de betrokkene deugdelijk vaststelt voordat inzage wordt verleend en (ii) verstrekking op begrijpelijke wijze dient op begrijpelijke wijze plaats te vinden. Het verlenen van inzage op afstand langs elektronische weg is eveneens toegestaan, mits daarbij verzekerd is dat de identiteit van de betrokkene deugdelijk kan worden vastgesteld.

Het ten behoeve van IRMA ophalen van de attributen bij de gemeente voldoet in onze optiek aan de door de Wet BRP gestelde minimumvereisten. De identiteit van de gebruiker wordt middels DigiD (met sms-verificatie) deugdelijk vastgesteld en de gegevens worden vervolgens via elektronische weg op afstand – en bovendien in begrijpelijke vorm – via IRMA aan de gebruiker verstrekt.<sup>30</sup> De door IRMA gehanteerde werkwijze van het ophalen van attributen is daarmee in lijn met de Wet BRP.

Wij benadrukken tot slot dat eenmaal opgehaalde attributen die staan opgeslagen in de IRMA-app op de smartphone van de gebruiker niet langer vallen onder de reikwijdte van de Wet BRP. De persoonsgegevens in de IRMA-app vallen uitsluitend onder de reikwijdte van de AVG, waarbij zich overigens de bijzondere situatie voordoet dat dat de persoonsgegevens in de IRMA-app slechts door de *gebruiker* worden vewerkt en niet door andere partijen.

<sup>28</sup> Artikel 2.53 eerste en tweede lid Wet BRP jo. artikel 2.55, eerste lid, Wet BRP. *Kamerstukken II 2011/12, 33 219, nr. 3, p. 44: "In de eerste plaats wordt het voor de ingeschrevene mogelijk om een verzoek tot inzage in de over hem opgenomen gegevens en het verkrijgen van een afschrift daarvan, in het vervolg te richten tot het college van burgemeester en wethouders van iedere willekeurige gemeente."*

<sup>29</sup> De verstrekking van attributen die plaatsvindt ten behoeve van IRMA is in dit licht een verstrekking 'light'. Er wordt immers geen volledig overzicht getoond, maar slechts een overzicht van een beperkte set persoonsgegevens.

<sup>30</sup> Wij merken (ten overvloede) op dat de bevoegdheid van artikel 2.55 Wet BRP strekt tot het kunnen controleren van de juistheid van de BRP-gegevens. Strikt genomen wordt het inzagerecht van artikel 2.55 Wet BRP in het geval van IRMA gebruikt voor een ander doel, namelijk het uploaden van attributen ten behoeve van IRMA. Wij achten dit niet onrechtmatig. Het is immers nu ook al het geval dat de burger na het verkrijgen van zijn BRP-gegevens de vrijheid heeft om zijn persoonsgegevens naar eigen inzicht te gebruiken. Hieruit volgt dat het de burger evenzeer vrijstaat om de van de gemeente verkregen BRP-gegevens ten behoeve van IRMA te verwerken.



### ***Ad (b) De gebruiker en de controleur***

- 3.3.5 Ook in de relatie tussen de gebruiker en de controleur, bestaat een wettelijke grondslag voor het verwerken van persoonsgegevens door de gemeente, nu in haar rol als controleur. Wij achten het in het belang van de publieke taak van de gemeente om – voorafgaand aan het aanbieden van gemeentelijke diensten of producten – de identiteit van de betrokkene vast te stellen. Een controle op de identiteit van de betrokkene via IRMA is noodzakelijk om te bewerkstelligen dat de gemeente de gemeentelijke diensten en producten aan de juiste persoon levert. Wij menen dan ook dat artikel 6, eerste lid, aanhef en onder e, AVG een wettelijke grondslag kan vormen voor de gegevensuitwisseling tussen de gemeente en de gebruiker.<sup>31</sup>
- 3.3.6 Tijdens de bespreking van 22 december met de gemeente, is expliciet aan bod gekomen of ook de toestemming van de gebruiker een wettelijke grondslag kan vormen voor de gegevensverstrekking aan de gemeente (artikel 6, eerste lid, aanhef en onder a, AVG).<sup>32</sup> De IRMA-app is zo vormgegeven dat de gebruiker steeds expliciete toestemming geeft voordat de persoonsgegevens aan de controleur (in dit geval de gemeente) wordt verstrekt. De vraag rijst of deze toestemming toereikend is in het licht van artikel 6 AVG.
- 3.3.7 De door IRMA gehanteerde werkwijze voor het verlenen van toestemming voldoet in zijn algemeenheid aan de volgende cumulatieve minimumvoorwaarden die de AVG aan de toestemming stelt:

(a) *de toestemming moet vrijelijk zijn gegeven*

De gebruiker dient daadwerkelijk een vrije keuze te hebben gehad of hij instemt met de verwerking van zijn attributen door de gebruiker.<sup>33</sup>

(b) *de toestemming moet specifiek zijn*

Het moet voor de gebruiker voorafgaand aan het verstrekken van zijn attributen duidelijk zijn voor welke doeleinden hij toestemming verleent voor het door de controleur verwerken van zijn persoonsgegevens. Het doel van de verwerking moet specifiek staan beschreven in de privacyverklaring van de controleur.

<sup>31</sup> Het gaat in dit geval om het BSN. Zoals wij hierna zullen toelichten, vormt artikel 10 Wvba een specifieke wettelijke grondslag voor de gemeente om het BSN van burgers te verwerken.

<sup>32</sup> De definitie van toestemming is opgenomen in artikel 4, aanhef en onder 11, AVG: "toestemming" van de betrokkene: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt".

<sup>33</sup> Vgl. Overwegingen 42 AVG: "Toestemming mag niet worden geacht vrijelijk te zijn verleend indien de betrokkene geen echte of vrije keuze heeft of zijn toestemming niet kan weigeren of intrekken zonder nadelige gevolgen." Zie tevens: Artikel-29 Werkgroep, 'Guidelines on consent under Regulation 2016/679' van 10 april 2018, WP259 rev. 01, p. 5-6.

- (c) de gebruiker moet voorafgaand aan het verlenen van zijn toestemming zijn geïnformeerd

De betrokkene dient voorafgaand aan het verlenen van zijn toestemming uitvoerig door de controleur te zijn geïnformeerd over de beoogde verwerking, zodat hij een geïnformeerde beslissing kan maken of hij al dan niet zijn toestemming verleent. Ook hier geldt dat de inhoud van de privacyverklaring van de controleur bepalend zal zijn voor de vraag of aan deze (deel)voorwaarde voor toestemming wordt voldaan.

- (d) de toestemming moet op een ondubbelzinnige wijze zijn verkregen, door middel van een actieve handeling.

De toestemming van de gebruiker wordt via IRMA met een actieve handeling kenbaar gemaakt aan de controleur. IRMA voldoet daarmee aan deze deelvoorwaarde.

- 3.3.8 Wij menen in het licht van het voorgaande dat de toestemming van de gebruiker een voldoende wettelijke grondslag *kan* bieden voor het verwerken van de persoonsgegevens van de gebruiker, mits de gemeente in haar rol als controleur ervoor zorgt dat zij het gebruik van de verkregen attributen beperkt tot specifieke doeleinden (bijv. de identificatie van de betrokkene ten behoeve van de aanvraag van gemeente diensten en producten) en de gemeente de gebruiker tijdig informeert over de verwerking van persoonsgegevens. Ook moet de betrokkene de mogelijkheid hebben om zijn toestemming gemakkelijk in te trekken.

Dit gezegd hebbende, plaatsen wij wel een kanttekening bij de voorwaarde dat de toestemming van de gebruiker '*vrijelijk*' moet zijn gegeven. De Europese privacy toezichthouders<sup>34</sup>, waaronder de Autoriteit Persoonsgegevens ('AP'), zijn van oordeel dat toestemming van een burger in beginsel niet als wettelijke grondslag kan dienen indien de verwerkingsverantwoordelijke een overheidsorgaan is.<sup>35</sup> Achtergrond hiervan is dat de machtsverhouding tussen de overheid en de burger zal maken dat de burger zich in veel gevallen niet vrij zal voelen om zijn toestemming te weigeren.

Er bestaat aldus een risico dat de AP in het geval van de gemeente zal concluderen dat de toestemming van de gebruiker *geen* wettelijke grondslag kan vormen voor het verwerken de persoonsgegevens van de gebruiker in het geval de controleur een overheidsorgaan is. We achten dit risico echter beperkt. In het geval van IRMA achten wij het zeer verdedigbaar dat sprake is van vrijelijke toestemming van de gebruiker. Doorslaggevend daarbij is dat het gebruik van IRMA *optioneel* wordt

<sup>34</sup> De Europese privacy toezichthouders zijn verenigd in de European Data Protection Board. Voor de inwerking van de AVG was dit nog de Artikel-29 Werkgroep.

<sup>35</sup> Artikel-29 Werkgroep, Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679, WP259, p. 6 e.v.



aangeboden door de gemeente. De gebruiker kan op geheel vrijwillige basis gebruik maken van IRMA. De gebruiker behoudt de mogelijkheid om in plaats van IRMA gebruik te maken van DigiD indien hij of zij de gemeentelijke diensten en producten wenst af te nemen. De weigering gebruik te maken van IRMA en persoonsgegevens te verstrekken aan de controleur (gemeente) heeft geen nadelige gevolgen voor de gebruiker. In dit licht bezien, zien wij niet in waarom een burger zich gedwongen zou voelen om zijn toestemming te verlenen. Kort en goed lijkt artikel 6, eerste lid, aanhef en onder a, AVG in het concrete geval van IRMA, althans in zijn huidige opzet<sup>36</sup>, een afdoende wettelijke grondslag te vormen voor het verwerken van de persoonsgegevens van de gebruiker door de gemeente.

Om echter discussie te voorkomen, doet de gemeente er verstandig aan om voor wat betreft de wettelijke grondslag te verwijzen naar haar publieke belang bij het verwerken van de persoonsgegevens (artikel 6, eerste lid, aanhef en onder e, AVG) in combinatie met het hierna te bespreken artikel 10 Wet Algemene Bepalingen Burgerservicenummer.

#### *Bijzondere persoonsgegevens & het BSN*

- 3.3.9 We merken op dat hoewel op zichzelf een wettelijke grondslag lijkt te bestaan voor het verwerken van de normale persoonsgegevens van de gebruiker door de gemeente als controleur, dit nog niet maakt dat de gemeente ook bevoegd is tot het verwerken van attributen van de gebruiker die kwalificeren als bijzondere persoonsgegevens.

Bijzondere persoonsgegevens zijn persoonsgegevens die naar hun aard gevoelig zijn. De categorieën bijzondere persoonsgegevens staan limitatief opgesomd in artikel 9, eerste lid, van de AVG. Voorbeelden van bijzondere persoonsgegevens zijn gegevens over iemands ras, gezondheidsgegevens en gegevens met betrekking tot iemands seksueel gedrag. Zowel directe als indirecte bijzondere persoonsgegevens vallen onder de bescherming van artikel 9 AVG. Het verwerken van bijzondere persoonsgegevens is verboden, tenzij hiervoor een algemene of specifieke doorbrekingsgrond bestaat in de AVG (artikel 9, tweede lid, AVG en artikelen 22 tot en met 30 UAVG) of een bijzondere wet.

- 3.3.10 Voor zover wij kunnen overzien, kunnen er vooralsnog geen bijzondere persoonsgegevens als attributen worden ingeladen in de IRMA-app. Er worden momenteel dus geen bijzondere persoonsgegevens verwerkt binnen IRMA. Mocht dit in de toekomst veranderen dan dient altijd vooraf te worden nagegaan of een doorbrekingsgrond voor het verwerken van het attribuut voorhanden is.

<sup>36</sup> Dit zou kunnen veranderen indien het gebruik van IRMA verplicht wordt gesteld en de burger geen alternatieve methoden meer heeft om de gemeentelijke producten en diensten af te nemen. In dat geval zal de AP naar verwachting eerder concluderen dat geen sprake meer is van vrijwillige toestemming.

- 3.3.11 Een persoonsgegeven dat wél reeds zal worden verwerkt door de gemeente, en ook door de gemeente in haar rol als controleur van de gebruiker zal worden uitgegeven en opgevraagd, is het BSN. Een nationaal identificatienummer zoals het BSN wordt in de AVG niet langer aangemerkt als bijzonder persoonsgegeven, maar als een *gereguleerd* persoonsgegeven. Op grond van artikel 87 AVG mag de Nederlandse wetgever specifieke voorwaarden stellen aan het gebruik van het BSN. De Nederlandse wetgever heeft hieraan uitvoering gegeven door in artikel 46, eerste lid, UAVG te bepalen dat het gebruik van wettelijke identificatienummers in beginsel bij (formele) wet moet zijn voorgeschreven en slechts mag worden gebruikt ter uitvoering van de in de wet genoemde doelstellingen (artikel 46, eerste lid, UAVG).
- 3.3.12 De wetgever heeft met artikel 10 Wet algemene bepalingen burgerservicenummer ('Wabb') een algemene wettelijke grondslag gecreëerd voor overheidsorganen om het BSN te verwerken voor de uitvoering van hun publiekrechtelijk taak. Artikel 10 Wabb biedt in onze optiek een voldoende wettelijke basis voor de gemeente om in haar rol van controleur via de IRMA-app het BSN bij de gebruiker op te vragen, mits het BSN daadwerkelijk wordt opgevraagd ten behoeve van een aan de gemeente opgedragen taak. Een belangrijke uit de Wabb voortvloeiende verplichting is dat de gemeente, bij het als controleur ontvangen van het BSN, zich ervan vergewist dat het BSN betrekking heeft op de persoon wiens persoonsgegevens zij verwerkt (artikel 12 Wabb). Het is de vraag of de IRMA-app de gemeente hiertoe voldoende mogelijkheid biedt. Wij menen van wel. De gemeente controleert immers bij ontvangst van het BSN-attribuut de authenticatie daarvan.<sup>37</sup>

Wij benadrukken dat slechts een controleur die overheidsorgaan is, de algemene verwerkingsgrondslag van artikel 10 Wabb kan invoeren. Andere controleurs, niet zijnde overheidsorganen zullen geen wettelijke grondslag hebben om het BSN bij de gebruiker op te vragen en deze te verwerken, tenzij zij hiertoe op grond van een formele wet gerechtigd toe zijn. Wij menen dat de gemeente als uitgever van het BSN-attribuut en de Stichting de gezamenlijke verantwoordelijkheid hebben om de gebruiker te informeren dat hij zijn BSN niet hoeft te delen met instanties die niet bevoegd zijn om het BSN te verwerken.<sup>38</sup> Uit de IRMA-website maken wij op dat de Stichting hier reeds voor waarschuwt. Wij raden de gemeente aan bij deelname aan het IRMA-experiment een zelfde soort waarschuwing op haar website op te nemen.

<sup>37</sup> Het risico blijft bestaan dat degene die het attribuut toont, het BSN-attribuut onrechtmatig op zijn IRMA-app heeft gedownload, dan wel het BSN-attribuut toont door middel van een gestolen telefoon. Dit zou overigens veronderstellen dat deze derde de beschikking heeft over de PIN van de gebruiker. Howel partijen hierop alert dienen te zijn, is dit geen IRMA-specifiek risico. Dit gevaar kan zich immers thans ook al bij de identificatie via DigiD verwezenlijken.

<sup>38</sup> Deze guidance zou een plaats kunnen krijgen binnen de IRMA-app zelf, bijvoorbeeld door middel van een pop-up scherm.

### ***Ad (c) De gebruiker en de Stichting***

- 3.3.13 Tot slot de gegevensstroom die plaatsvindt tussen de gebruiker en de Stichting. Voor zover persoonsgegevens worden verwerkt, zou de wettelijke grondslag 'toestemming' een grondslag kunnen vormen (artikel 6, eerste lid, aanhef en onder a, AVG). Uiteraard dient ook deze toestemming te voldoen aan de hiervoor achter randnummer 3.3.7 beschreven minimumvoorwaarden. Wij merken op dat, anders dan in het geval van de gemeente, zich in dit geval vermoedelijk geen risico voordoet dat de toestemming van de gebruiker niet als 'vrijelijk' kan worden beschouwd. Er is immers geen sprake van een machtsverhouding tussen de Stichting en de gebruiker.

#### *Bijzondere persoonsgegevens en het BSN*

- 3.3.14 In de huidige opzet verwerkt de Stichting geen bijzondere persoonsgegevens en BSN. Zoals reeds besproken, zijn er op dit moment geen attributen die informatie bevatten over bijzondere persoonsgegevens. Dit kan mogelijk anders worden in het geval (nieuwe) uitgevers besluiten om bijzondere persoonsgegevens als attributen uit te geven.

### **3.4 Materiële eisen van de AVG**

- 3.4.1 Nu duidelijkheid is verkregen over de vraag in welke situaties sprake is van het verwerken van persoonsgegevens door de gebruiker, uitgever en controleur en in hoeverre daarvoor een wettelijke grondslag bestaat, rijst de vraag in of de verwerkingen van de persoonsgegevens van de gebruiker door middel van IRMA voldoen aan de materiële eisen van de AVG.
- 3.4.2 Tijdens de bespreking van 22 december 2018 heeft de gemeente aangegeven dat zij geen behoefte heeft aan een uitgebreide toets van alle materiële vereisten. De gemeente heeft ons gevraagd te toetsen of zich op grond van de AVG wezenlijke belemmeringen voordoen die zouden maken dat zou moeten worden afgezien van het IRMA experiment. Wij zullen in deze paragraaf doen ook enkel stilstaan bij de materiële vereisten die (voorafgaand aan de start van het IRMA-experiment) de bijzondere aandacht van de gemeente vereisen. Wij doen dit als volgt. Eerst zullen wij een algemeen overzicht geven van de materiële vereisten waaraan IRMA moet voldoen. Vervolgens zullen wij, voor zover de materiële vereisten van de AVG daartoe aanleiding geven, in paragraaf 3.4.4 e.v toelichten in hoeverre wij belemmeringen zien voor het gebruik van IRMA en/of de gemeente bepaalde acties zal moeten ondernemen om aan de materiële voorwaarden van de AVG te voldoen. Voor zover noodzakelijk, zullen wij ook aanbevelingen doen om ervoor te zorgen dat het IRMA-experiment in overeenstemming met de AVG plaatsvindt.

#### *Algemeen overzicht van de materiële vereisten van de AVG*

- 3.4.3 De AVG stelt – samengevat weergegeven – de volgende materiële vereisten aan de verwerking van persoonsgegevens:

- (*geautomatiseerde besluitvorming*) er vindt geen geautomatiseerde besluitvorming plaats, tenzij daarvoor een wettelijke grondslag bestaat (artikel 22 AVG jo. artikel 40 UAVG).
- (*internationale doorgifte*) de persoonsgegevens in IRMA worden niet buiten de EU doorgegeven, tenzij hiervoor een wettelijke grondslag bestaat (artikel 45 tot en met 49 AVG).

#### *Algemene beginselen*

- (*doelbindingsbeginsel*) de persoonsgegevens worden door middel van IRMA voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld. Daarnaast worden persoonsgegevens door controleurs en gebruikers niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen (artikel 5, eerste lid, aanhef en onder b, AVG en artikel 6, vierde lid, AVG).
- (*dataminimalisatie / noodzakelijkheidsbeginsel*) de persoonsgegevens mogen slechts worden verwerkt voor zover zij toereikend, ter zake dienend en niet bovenmatig zijn (artikel 5, eerste lid, aanhef en onder c, AVG)
- (*juist en actueel*) de persoonsgegevens dienen juist te zijn en zo nodig geactualiseerd te worden (artikel 5, eerste lid, aanhef en onder d, AVG).
- (*bewaartermijn*) de persoonsgegevens mogen door de controleur, de uitgever en de Stichting en door hen ingeschakelde derden niet langer worden bewaard dan noodzakelijk (artikel 5, eerste lid, aanhef en onder e, AVG).
- (*verantwoordingsplicht*) de verwerkingsverantwoordelijken die gebruik maken van IRMA en door hen ingeschakelde verwerkers moeten kunnen aantonen dat zij de beginselen voor de verwerking van persoonsgegevens naleven (artikel 5, tweede lid, AVG jo. artikel 24, eerste lid, AVG)
- *De rechten van de betrokkene*
  - (*informatieplicht*) de gebruiker van IRMA moet door de uitgever, controleur en de Stichting worden geïnformeerd over de verwerking van zijn persoonsgegevens (artikel 13 en 14 AVG).
  - (*recht op inzage*) IRMA maakt de uitoefening door de betrokkene van zijn recht op inzage mogelijk, althans belemmert deze niet (artikel 15 AVG).

- (*recht op correctie*) de gebruiker heeft op grond van artikel 16 AVG het recht om de verwerkingsverantwoordelijke om correctie van hem betreffende onjuiste persoonsgegevens te verkrijgen en om onvolledige persoonsgegevens aan te vullen (artikel 16 AVG).
- (*recht op wissing*) de gebruiker heeft in bepaalde gevallen het recht op wissing van hem betreffende persoonsgegevens (artikel 17 AVG).
- (*recht op beperking van de verwerking*) de gebruiker heeft het recht op beperking van de verwerking in de in artikel 18, eerste lid, AVG genoemde gevallen (artikel 18 AVG).
- (*recht op overdraagbaarheid*) IRMA maakt, voor zover dit wettelijk is vereist, de uitoefening van het recht op overdraagbaarheid mogelijk (artikel 20 AVG)
- (*recht op bezwaar*) IRMA vormt geen belemmering voor de uitoefening van het recht op bezwaar (artikel 21 AVG).

*Eisen met betrekking tot de beveiliging van de persoonsgegevens*

- (*privacy by design & default*) het ontwerp en het gebruik van IRMA moet in overeenstemming zijn met de beginselen van privacy by design en default (artikel 25 AVG)
- (*passende beveiligingsmaatregelen*) IRMA is passend beveiligd en de gemeente zorgt als uitgever en controleur dat de uitgegeven respectievelijk verkregen persoonsgegevens eveneens passend beveiligd zijn (artikel 5, eerste lid, aanhef en onder f, AVG jo. artikel 32 AVG). Ook door de controleur, uitgever en Stichting ingeschakelde derden dienen passende beveiligingsmaatregelen te treffen.
- (*meldplicht datalekken*) er zijn heldere afspraken over de wijze waarop datalekken moeten worden gemeld aan de Autoriteit Persoonsgegevens en/of gebruikers (artikel 33 en 34 AVG).
- (*Privacy Impact Assessment*) er wordt een PIA verricht voor zover de verwerking die plaatsvindt via IRMA een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen (artikel 35 AVG)

### **Analyse van de materiële vereisten van de AVG / Aanbevelingen**

- 3.4.4 De vraag rijst in hoeverre de hiervoor beschreven materiële vereisten van de AVG een belemmering vormen voor het gebruik van IRMA en/of de gemeente actie zal moeten ondernemen om aan de materiële voorwaarden van de AVG te voldoen. Zoals gezegd, zullen wij niet iedere voorwaarde uitgebreid toelichten. Wij beperken ons tot de punten die de aandacht vereisen van de gemeente. De materiële vereisten van de AVG waar wij geen problemen of belemmeringen hebben geconstateerd, zullen wij in deze paragraaf onbesproken laten.
- 3.4.5 Wij stellen voorop dat wij bij het verrichten van de analyse van IRMA geen wezenlijke belemmeringen hebben geconstateerd voor het van start gaan met het IRMA-experiment. IRMA voldoet in hoofdlijnen aan de materiële voorwaarden van de AVG. Dit neemt niet weg dat er enkele aandachtspunten zijn waarvan de gemeente en de Stichting zich bewust moeten zijn voordat zij van start gaat met het IRMA-experiment. Hieronder volgt een opsomming van de aandachtspunten die wij bij het gebruik van IRMA constateren. Wij zullen daarbij steeds, voor zover noodzakelijk, een aanbeveling doen op welke wijze eventuele belemmeringen verholpen kunnen worden.

#### **Aandachtspunt – Geautomatiseerde besluitvorming**

*De gemeente dient er alert op te zijn dat het gebruik van IRMA in specifieke situaties zal kunnen worden aangemerkt als (een onderdeel van) geautomatiseerde individuele besluitvorming.<sup>39</sup> Dit kan in strijd zijn met de AVG en de UAVG (artikelen 22 AVG en artikel 40 Uitvoeringswet AVG). Het verdient aanbeveling om bij iedere uitbreiding van de inzet van IRMA na te gaan of het gebruik van IRMA mogelijk wordt ingezet ten behoeve van geautomatiseerde besluitvorming en zo ja, of daarvoor een wettelijke grondslag bestaat. Wij raden de gemeente aan om in haar rol als controleur zoveel mogelijk te voorkomen dat IRMA wordt gebruikt ten behoeve van individuele besluitvorming, dan wel het gebruik van IRMA te beperken tot zogenaamde gebonden beschikkingen.*

#### *Toelichting*

- 3.4.6 Op grond van artikel 22, eerste lid, AVG mag niemand worden onderworpen aan een besluit dat uitsluitend is gebaseerd op geautomatiseerde verwerking van persoonsgegevens, waaronder profilering, dat rechtsgevolgen voor hem heeft of hem in aanmerkelijke mate treft (hierna: geautomatiseerde besluitvorming). Dit verbod heeft betrekking op louter geautomatiseerde besluitvorming, dus besluitvorming zonder menselijke tussenkomst. In de memorie van toelichting bij de Uitvoeringswet AVG worden verschillende voorbeelden van geautomatiseerde besluitvorming genoemd, waaronder het toekennen van kinderbijslag, het

<sup>39</sup> Bijvoorbeeld in het geval dat het tonen van attribuut (bijv. leeftijd) door de gebruiker aan de gemeente er geautomatiseerd toe leidt dat een aanvraag voor toeslag wordt afgewezen. IRMA wordt aldus geïntegreerd in het geautomatiseerde besluitvormingsproces en is daarmee medebepalend voor de uitkomst van het geautomatiseerde besluitvormingsproces.



bijstellen van de hoogte van het recht op studiefinanciering op basis van veranderingen in het inkomen van een van de ouders of het zonder menselijke tussenkomst vaststellen van een overtreding van de maximumsnelheid (*Kamerstukken II 2017/18, 34 851, nr. 3, p. 120-121*). Het begrip 'besluit' heeft zowel betrekking op publieke als op private besluiten (*Kamerstukken II 2017/18, 34 851, nr. 3, p. 46*).

- 3.4.7 In artikel 22, tweede lid, AVG zijn drie uitzonderingen opgenomen op het verbod op geautomatiseerde besluitvorming. Het verbod geldt niet als het besluit (kort gezegd):
- a. noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke;
  - b. is toegestaan bij een Unierechtelijke of nationale bepaling; of
  - c. berust op de nadrukkelijke toestemming van de betrokkene.
- 3.4.8 In artikel 40 UAVG is de afwijkingsmogelijkheid onder b) nader uitgewerkt. Artikel 40 UAVG bepaalt dat het verbod op geautomatiseerde besluitvorming niet geldt voor zover het gaat om een geautomatiseerde individueel besluit dat door de verwerkingsverantwoordelijke wordt genomen om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust of noodzakelijk is voor de vervulling van een taak van algemeen belang. Het gaat hier om zogenaamde gebonden besluiten, waarbij een zeer geringe beoordelingsruimte bestaat. Bij dergelijke besluiten heeft menselijke tussenkomst in beginsel geen meerwaarde. Hierbij kan volgens de wetgever gedacht worden aan onder meer het toekennen van kinderbijslag en het bijstellen van de hoogte van het recht op studiefinanciering op basis van veranderingen in het inkomen van een van de ouders.<sup>40</sup>
- 3.4.9 Hoewel IRMA geen middel is voor individuele geautomatiseerde besluitvorming, kan IRMA wel ten behoeve daarvan worden ingezet. De contoleur kan IRMA incorporeren in het geautomatiseerde besluitvormingsproces. Gedacht kan worden aan de situatie dat een contoleur via IRMA vraagt om een leeftijdsattribuut (bijv. 65+) voor een bepaalde toeslag en zijn systeem zo heeft ingesteld dat het tonen van een afwijkende leeftijd geautomatiseerd leidt tot afwijzing van de aanvraag, zonder dat daarbij een menselijke heroverweging plaatsvindt.
- 3.4.10 Wij raden de gemeente aan om in haar rol als controleur zoveel mogelijk te voorkomen dat IRMA wordt gebruikt ten behoeve van individuele besluitvorming, dan wel het gebruik van IRMA te beperken tot zogenaamde gebonden beschikkingen. Wil de gemeente IRMA toch ten behoeve van individuele geautomatiseerde besluitvorming inzetten kan zij hier slechts toe overgaan indien sprake is van een gebonden beschikking en de individuele geautomatiseerde besluitvorming plaatsvindt ter uitvoering van een wettelijke plicht of noodzakelijk is voor de uitvoering een taak van algemeen belang. Dit dient per concreet geval te worden beoordeeld.

<sup>40</sup> *Kamerstukken II 2017/18, 34 851, nr. 3, p. 105.*

Bovengenoemd risico doet zij bij de door de gemeente beoogde toepassingen van IRMA (nog) niet voor. Naar wij begrijpen zal de gemeente als controleur IRMA vooralsnog slechts gaan gebruiken als (optioneel) identificatiemiddel. Nadat de burger zich met IRMA op de gemeentelijke website heeft geïdentificeerd, verkrijgt hij de mogelijkheid om gemeentelijke diensten en/of producten aan te vragen. Van geautomatiseerde besluitvorming is geen sprake. De gemeentelijke dienst die wordt geleverd is immers niet gekoppeld aan de attributen die door IRMA worden getoond. Daarbij geldt bovendien dat de beoordeling niet louter geautomatiseerd plaatsvindt. Dit kan in de toekomst echter veranderen, hetgeen ook de reden vormt dat wij de gemeente nu al wijzen op de mogelijke risico's.

- 3.4.11 Als een geautomatiseerd besluit wordt genomen op grond van één van de uitzonderingsgronden moet de gemeente passende maatregelen treffen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene. Daarvoor moet in ieder geval het recht op menselijke tussenkomst, het recht voor een betrokkene om zijn standpunt kenbaar te maken en het recht om het besluit aan te vechten, zijn geborgd (artikel 22, derde lid, AVG en artikel 40, derde lid, UAVG).

**Aandachtspunt – Risico op onjuiste en niet actuele attributen**

*Hoewel de attributen/credentials bij uitgifte worden gewaarmerkt met een digitale handtekening die de controleur bij ontvangst van de attributen van de gebruiker kan controleren, is niet met zekerheid te zeggen of de informatie de persoonsgegevens juist en actueel zijn. De door de gebruiker opgehaalde attributen kunnen inmiddels zijn verouderd. Dit is een inherent risico is aan het gebruik van IRMA. De uitgever kan dit risico enigszins beperken door een geldigheidsdatum te zetten op de door de gebruiker opgehaalde attributen. Het is uiteindelijk de verantwoordelijkheid van de gebruiker om bij wijziging van zijn persoonsgegevens zijn attributen te verversen. Dit neemt niet weg dat een gebruiker (voor wat betreft zijn BRP-gegevens), gelet op de huidige instelling van IRMA, circa drie maanden lang zijn verouderde persoonsgegevens via IRMA zou kunnen tonen. Het is aldus mogelijk dat een controleur bij ontvangst van attributen niet actuele persoonsgegevens ontvangt en verwerkt.<sup>41</sup> De gemeente moet op dit risico bedacht zijn. Naar wij begrijpen kan de gemeente ervoor kiezen om een korte (houdbaarheids)termijn te hanteren. De gemeente zou aldus, indien zij dit noodzakelijk acht, een strengere termijn kunnen hanteren.*

<sup>41</sup> Het is uiteraard afhankelijk van de aard van het attribuut of het attribuut kan verouderen. Zo zal het BSN nooit veranderen en doet zicht ten aanzien van dit attribuut ook geen risico voor dat de juistheid van dit attribuut wordt aangetast. Hetzelfde geldt voor de geboortedatum van de betrokkene.

### **Aandachtspunt – Noodzakelijkheidsbeginsel / dataminimalisatie**

*De verwerking van persoonsgegevens moet toereikend zijn, ter zake dienend een beperkt zijn tot wat strikt noodzakelijk is voor de doeleinden waarvoor de persoonsgegevens worden verwerkt (dataminimalisatie).<sup>42</sup> Deze verplichting houdt kortgezegd in dat een controleur (dit kan de gemeente of een andere controleur zijn) bij het gebruik van IRMA niet meer attributen bij de gebruiker mogen worden opgevraagd dan strikt noodzakelijk voor het beoogde doel van de IRMA-sessie. Dit betreft een eigen verantwoordelijkheid van de controleur, aangezien die zelfstandig bepaalt welke attributen bij de gebruiker worden opgevraagd en welke attributen zij accepteert als voldoende actueel. Ook dient de gemeente een strikte bewaartermijn te hanteren voor verkregen attributen. De gemeente dient in haar rol als controleur zich steeds bewust te zijn van het feit dat zij de IRMA-uitvraag beperkt tot het strikt noodzakelijke. Doet zij dit niet, dan bestaat het risico dat ze daarmee in strijd handelt met het beginsel van dataminimalisatie. Wij zien hier ook een rol weggelegd bij de Stichting. Indien de Stichting op de hoogte raakt dat een controleur onnodig veel attributen opvraagt bij de gebruiker, dan zou de Stichting die controleur daarop moeten aanspreken. Het verdient aanbeveling om de gebruiker de mogelijkheid te bieden om bij de controleur een klacht in te dienen, zodat deze maatregelen kan treffen. Daarmee kan mogelijk ook worden voorkomen dat de gebruiker zich wendt tot de Autoriteit Persoonsgegevens.*

### **Actie gemeente – Vaststellen bewaartermijn**

*De gemeente moet op grond van artikel 5, eerste lid, aanhef en onder e, AVG een bewaartermijn vaststellen op het verwerken van attributen die zij in haar rol als controleur van de gebruiker verkrijgt. De gemeente dient daarbij als uitgangspunt te nemen dat de bewaartermijn niet langer dan noodzakelijk mag zijn voor de verwerking van de doeleinden waar zij de attributen heeft verkregen en verwerkt.<sup>43</sup>*

### **Actie gemeente – Verantwoord IRMA in het verwerkingsregister en privacybeleid en privacy protocollen**

*De gemeente dient in het licht van de verantwoordingsplicht van artikel 5, tweede lid, AVG een verwerkingsregister bij te houden. Daarnaast dient de gemeente een algemeen privacybeleid te hanteren dat concreet is uitgewerkt in privacyprotocollen. We gaan er van uit dat de gemeente reeds beschikt over deze verantwoordingsmiddelen. De gemeente zal de verwerkingen die plaatsvinden bij de uitgifte en de controle van attributen/credentials via IRMA moeten verantwoorden in haar verwerkingsregister, privacybeleid en protocollen. De gemeente zou in een privacyprotocol kunnen concretiseren op welke wijze de gemeente omgaat met de persoonsgegevens die zij via het gebruik van IRMA over de gebruiker verkrijgt. In het bijzonder dient de gemeente te beschrijven welke bewaartermijn zij hanteert voor attributen die zij van de gebruiker verkrijgt en/of zij al dan niet aanvullende persoonsgegevens (zoals IP-adressen) van de gebruiker wil verwerken. Het verdient aanbeveling om dit voorafgaand aan de start van het IRMA-experiment te doen.*

<sup>42</sup> Artikel 5, eerste lid, aanhef en onder c, AVG.

<sup>43</sup> Artikel 5 van de AVG.

### **Actie gemeente – Stel een op IRMA toegespitste privacyverklaring op**

*De gemeente zal op grond van artikel 13 AVG de gebruiker voorafgaand aan de verwerking moeten informeren over de verwerking van de persoonsgegevens van de gebruiker. Dit is met name relevant voor zover de gemeente optreedt als controleur. De gemeente zal een op IRMA toegespitste privacyverklaring moeten opstellen. Deze privacyverklaring zal de volgende informatie moeten bevatten:*

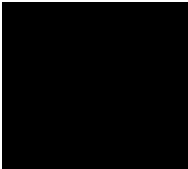
- i. de identiteit en contactgegevens van de (Functionaris Gegevensbescherming van de) gemeente en, indien aan de orde, van zijn vertegenwoordiger;*
- ii. de doelen waarvoor de persoonsgegevens worden verwerkt en de rechtsgrond van de verwerking;*
- iii. de (categorieën van) ontvangers (waaronder de inzet van verwerkers);*
- iv. eventuele doorgifte van persoonsgegevens aan een derde land;*
- v. de bewaartermijn;*
- vi. de rechten van de betrokkene;*
- vii. het recht van de betrokkene om een klacht in te dienen bij de AP;*
- viii. dat de betrokkene het recht heeft de verleende toestemming te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan; en*
- ix. het bestaan van geautomatiseerde besluitvorming.<sup>44</sup>*

*De gemeente dient de privacyverklaring aan de gebruiker beschikbaar te stellen voorafgaand aan de verwerking van de persoonsgegevens. Wij raden dan ook aan om een link naar de privacyverklaring op te nemen op de webpagina van de gemeente, meer concreet op (i) de pagina waar de gebruiker kan verzoeken om uitgifte van zijn persoonsgegevens en (ii) de pagina waar de gebruiker via IRMA zijn persoonsgegevens aan de gemeente kan verstrekken.*

*Wij constateren tot slot dat de Stichting voor de IRMA-app reeds beschikt over een privacyverklaring. De privacyverklaring wordt aan de gebruiker aangeboden in de IRMA-app (onder het kopje 'Over IRMA'). Hoewel op hoofdlijnen correct, is de privacyverklaring op aspecten onvolledig. Momenteel ontbreekt er een passage over de rechten van de betrokkene (recht op inzage, correctie of wissing van de persoonsgegevens, evenals het recht op overdraagbaarheid). Het verdient aanbeveling om de huidige privacyverklaring van de Stichting op dit punt uit te breiden.*

### **Aandachtspunt – De rechten van de betrokkene**

<sup>44</sup> Wij noemen hier slechts de uit artikel 13 AVG voortvloeiende informatieonderdelen die voor de gemeente bij het gebruik van IRMA relevant zijn. Artikel 13 AVG noemt nog meer informatieonderdelen (zoals bijvoorbeeld de verplichting om de betrokkene te informeren of de verstrekking een wettelijke of contractuele verplichting is dan wel een noodzakelijk voorwaarde is om een overeenkomst af te sluiten, en of de betrokkene verplicht is om de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer deze niet worden verstrekt). Deze situatie doet zich in geval van IRMA niet voor (de verwerking strekt niet tot een wettelijke of contractuele verplichting). Voor een volledige opsomming verwijzen wij naar de tekst van artikel 13 AVG.



*Zoals reeds toegelicht heeft de betrokkene op grond van de AVG diverse rechten, onder meer het recht op inzage, correctie, wissing en het recht op overdraagbaarheid. De IRMA-app belemmert de uitoefening van de rechten van de betrokkene niet. De gemeente zal per concreet verzoek moeten beoordelen of en zo ja, op welke wijze wordt voldaan aan het verzoek van de gebruiker. Wij wijzen er overigens wel op dat het voor de gebruiker duidelijk moet zijn tot wie hij zijn verzoeken kan richten. De gebruiker kan bij de uitgever en controleur (in beide gevallen de gemeente) zijn rechten uitoefenen voor zover er persoonsgegevens worden verwerkt bij de uitgifte respectievelijk controle van de attributen door de gemeente.<sup>45</sup> Wil de gebruiker informatie over de persoonsgegevens die in het kader van zijn IRMA-account worden verwerkt dan dient hij zijn verzoek te richten tot de Stichting.<sup>46</sup>*

*Wij benadrukken dat de betrokkene zijn rechten alleen kan uitoefenen indien de gemeente / de Stichting daadwerkelijk persoonsgegevens verwerkt. Zoals toegelicht achter paragraaf 2.1 van dit rapport, is er niet in alle gevallen sprake van het verwerken van persoonsgegevens. Denk bijvoorbeeld aan de situatie dat de gemeente een niet-identificeerbaar attribuut van de gebruiker ontvangt en daarbij geen aanvullende persoonsgegevens van de gebruiker verwerkt (bijv. IP-adres). De gegevens die de gemeente daarmee ontvangt zijn niet herleidbaar tot de gebruiker. Ontvangt de gemeente in een dergelijk geval een verzoek van de gebruiker, dan kan de gemeente het verzoek weigeren. Zoals volgt uit artikel 11, eerste lid, AVG is de gemeente niet verplicht om aanvullende gegevens bij te houden, te verkrijgen of te verwerken om de identificatie van de betrokkene toch mogelijk te maken. De gemeente is slechts verplicht om een verzoek in behandeling te nemen, indien de betrokkene aanvullende gegevens verstrekt die het mogelijk maken hem te identificeren (bijv. het tijdstip van de transactie en/of zijn IP-adres).<sup>47</sup>*

#### **Aandachtspunt – De beveiliging van IRMA**

*Voor zover wij kunnen overzien, lijkt IRMA een passend beveiligingsniveau te bieden. IRMA lijkt daarmee te voldoen aan de vereisten van de AVG. Volledige zekerheid kunnen wij echter niet geven. Daarvoor is een uitvoerige technische audit vereist, dat zoals gezegd, buiten onze expertise valt. Enig aandachtspunt is dat IRMA momenteel nog geen back-up mogelijkheid aanbiedt en daardoor mogelijk niet wordt voldaan aan de (beveiligings)voorwaarde dat bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig moet kunnen worden hersteld. In de huidige situatie kan de gebruiker de app slechts blokkeren, opnieuw een account aanmaken en vervolgens wederom alle attributen opvragen bij de uitgevers. De Stichting werkt momenteel aan het aanbieden van een back-up mogelijkheid.*

<sup>45</sup> Hierbij zij benadrukt dat de gemeente en de Stichting geen toegang hebben tot de persoonsgegevens in de IRMA-app. Deze persoonsgegevens vallen onder de regie van de betrokkene. Dit maakt aldus dat de rechten van de betrokkene zich niet uitstrekken tot de persoonsgegevens die hij zelfstandig in de app beheert.

<sup>46</sup> Het gaat hier in beginsel om het persoonlijke e-mailadres van de gebruiker, de attributen van de gebruiker voor zover de Stichting als verwerker voor de uitgever optreedt en het IP-adres in probleemrapporten.

<sup>47</sup> Artikel 11, tweede lid, AVG.



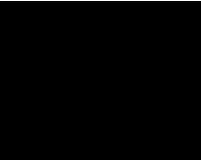
### *Toelichting*

- 3.4.12 Op grond van artikel 5, eerste lid, aanhef en onder f, AVG moeten door het nemen van passende technische of organisatorische maatregelen de persoonsgegevens op een dusdanige manier worden verwerkt dat een passende beveiliging van de persoonsgegevens is gewaarborgd en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.
- 3.4.13 Op grond van artikel 32 AVG moet de verwerkingsverantwoordelijke, rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, passende technische en organisatorische maatregelen nemen om een op het risico afgestemd beveiligingsniveau te waarborgen. Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte Persoonsgegevens, hetzij per ongeluk hetzij onrechtmatig. Waar passend, omvatten de beveiligingsmaatregelen onder meer het volgende:
- a. de pseudonimisering en versleuteling van persoonsgegevens;
  - b. het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
  - c. het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
  - d. een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

IRMA moet voldoende beveiligd zijn en de verwerkingsverantwoordelijken (uitgever, controleur en de Stichting) moeten erop toezien dat dat het geval is. Bij de beoordeling zal onder meer een rol kunnen spelen of de [Richtsnoeren Beveiliging Persoonsgegevens](#) in acht zijn genomen. Voor wat betreft de vraag of de versleuteling adequaat is, wijzen wij de door de Artikel-29 Werkgroep opgestelde [Richtlijn inzake de meldplicht datalekken](#). Om te kunnen vaststellen of voldoende passende waarborgen zijn getroffen ter beveiliging van de persoonsgegevens in IRMA is een technische audit vereist. Dit valt buiten onze expertise. Dit neemt niet weg dat wij globaal kunnen toetsen of de gekozen beveiligingsmaatregelen opvallende gebreken vertonen met de wettelijke voorgeschreven beveiligingsnormen.

3.4.14 De Stichting heeft de technische, organisatorische en juridische maatregelen opgenomen in haar beveiligingsbeleid en protocollen.<sup>48</sup> Hieronder volgt een (niet-uitputtende) opsomming van de belangrijkste beveiligingsaspecten van IRMA:

- IRMA maakt gebruik van een (Idemix) keyshare server. Kortgezegd houdt dit in dat de gebruiker een geheime sleutel verkrijgt die noodzakelijk is voor het ophalen en uitgeven van attributen. Deze sleutel wordt gesplitst. Een deel van de sleutel (de private key) staat opgeslagen in de app. Het andere deel van die sleutel staat opgeslagen op de keyshare server die wordt beheerd door de Stichting. Het uitgeven van attributen kan alleen plaatsvinden als de gebruiker zijn juiste pincode invoert en de beide delen van de sleutels verbinding met elkaar maken (*proof of knowledge*).
- De gebruiker dient bij het ophalen en uitgeven van zijn attributen steeds gebruik te maken van een persoonlijke PIN waarover alleen hij de beschikking heeft. De juistheid van de PIN wordt per transactie geverifieerd door de Keyshare server. Wordt de PIN meer dan drie keer onjuist opgegeven, dan wordt de IRMA sessie tijdelijk (met exponentieel oplopende timeout per foute poging) geblokkeerd. Op de gebruiker rust de verantwoordelijkheid om zijn PIN geheim te houden.
- Alleen de uitgever kan als houder van de Idemix private key credentials/attributen uitgeven die door de Idemix public key kunnen worden geverifieerd (*credential unforgeability*).
- De betrouwbaarheid en juistheid van de attributen is in belangrijke mate afhankelijk van de wijze waarop de gebruiker zijn attributen bij uitgevers kan ophalen. Dit verschilt per uitgever. Zo dient de gebruiker bij het ophalen van zijn BRP-gegevens bij de gemeente zijn DigiD op te geven. In andere gevallen zal het opgeven van een naam en wachtwoord voldoende zijn (bijv. het ophalen van social netwerk-attributen). Dit betreft in vergelijking met DigiD een minder betrouwbare manier van het vaststellen van de identiteit van de betrokkene. Attributen die zien op de financiële gegevens van de gebruiker kunnen via iDeal en iDIN worden opgehaald. Dit is vele malen betrouwbaarder dan het enkele opgeven van een gebruikersnaam en wachtwoord, omdat in het geval van iDeal sprake is van twee factor authenticatie.
- De controleur kan achteraf bij het doorlopen van meerdere IRMA sessies en het verkrijgen van attributen niet vaststellen of de verkregen attributen van dezelfde gebruiker zijn verkregen. De IRMA-sessies zijn niet met elkaar te koppelen (*multi-show unlinkability*). Dit is slechts anders indien de uitgever



ook aanvullende persoonsgegevens verwerkt waardoor de IRMA-sessies toch herleidbaar worden tot een gebruiker (IP-adres en MAC adres<sup>49</sup>).

- Het tonen van de IRMA attributen door de gebruiker aan de controleur vindt zonder tussenkomst van een derde centrale partij plaats. Hierdoor wordt voorkomen dat er een privacy hotspot ontstaat dat gemakkelijk vatbaar is voor beveiligingsinbreuken.
- De gebruiker heeft de mogelijkheid om zelfstandig via MijnIRMA de IRMA-app te blokkeren in geval zijn smartphone is gestolen of verloren. Eenmaal geblokkeerd, blijven de attributen weliswaar opgeslagen op de IRMA-app, maar kunnen de attributen niet meer worden gebruikt om een transactie te verrichten. Doordat het IRMA-account is geblokkeerd via MijnIRMA, kan niet langer een cryptografisch geldige verstreking worden gegenereerd en zijn de IRMA-attributen vanaf dat moment onbruikbaar.
- De Stichting kan eveneens een IRMA-account blokkeren. Zij gaat hiertoe over indien uit de loggegevens van een account blijkt dat het aantal IRMA onevenredig veel wordt gebruikt. Het IRMA-account zal dan veiligheidshalve worden beveiligd.
- Het is momenteel nog niet mogelijk om een back-up van het account te verkrijgen, dit betekent dat de gebruiker na het blokkeren van zijn account opnieuw een account zal moeten aanmaken en opnieuw alle attributen zal moeten ophalen. De Stichting is voornemens om deze backup mogelijkheid te gaan aanbieden.

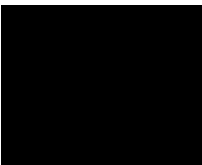
3.4.15 Bovengenoemde beveiligingsmaatregelen overzien, lijkt, voor zover wij kunnen vaststellen, IRMA een passend beveiligingsniveau te hanteren. Volledige zekerheid kunnen wij echter niet geven. Daarvoor is een uitvoerige technische audit vereist, hetgeen zoals gezegd, buiten dit advies en onze expertise valt. Enig aandachtspunt is dat IRMA momenteel nog geen back-up mogelijkheid aanbiedt en daardoor mogelijk niet wordt voldaan aan de (beveiligings)voorwaarde dat bij 'een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig moet kunnen worden hersteld'. In de huidige situatie kan de gebruiker de app slechts blokkeren, opnieuw een account aanmaken en vervolgens wederom alle attributen opvragen bij de uitgevers. De Stichting werkt momenteel aan het aanbieden van een back-up mogelijkheid.

### **Conclusie**

3.4.16 Tot zover onze analyse van de materiële vereisten van IRMA. Wij hebben geconcludeerd dat er geen wezenlijke belemmeringen zijn om van start te gaan met het IRMA-experiment. In dit hoofdstuk hebben wij echter wel enkele aandachtspunten voor de gemeente geconstateerd en, voor zover nodig, enkele aanbevelingen gedaan. We raden de gemeente

<sup>49</sup> Het MAC-adres staat voor 'media acces control' en is een uniek identificatienummer van de smartphone of het apparaat van de gebruiker waar de IRMA-app staat opgeslagen.





aan om uitvoering te geven aan deze aanbevelingen voordat van start wordt gegaan met de pilot.

#### **4 IRMA en de overige wetgeving**


- 4.1.1 In het voorgaande hoofdstuk zijn wij ingegaan op de vraag of IRMA voldoet aan de vereisten van de AVG. Doordat IRMA mede als elektronische identificatietool zal worden gebruikt, dient de gemeente bij het gebruik van IRMA (naast de AVG) tevens te voldoen aan de wettelijke regels die gelden voor elektronische identificatiemiddelen. Wij belichten in verband daarmee hierna de eIDAS-verordening<sup>50</sup> en het Wetsvoorstel Wet Digitale Overheid.

#### **4.2 De eIDAS-verordening**

- 4.2.1 De Europese eIDAS-verordening is sinds 1 juli 2016 van kracht. eIDAS staat voor 'Electronic Identities And Trust Services'. Met eIDAS hebben de Europese lidstaten afspraken gemaakt om dezelfde begrippen, betrouwbaarheidsniveaus en onderlinge digitale infrastructuur te gebruiken. De regels van de eIDAS-verordening over de vereiste betrouwbaarheid van identificatiemiddelen is nader uitgewerkt in de Uitvoeringsverordening 2015/1502.<sup>51</sup> Doel van de verordening is het vertrouwen in elektronische transacties te vergroten door te voorzien in een gemeenschappelijke grondslag voor veilige elektronische interactie tussen burgers, bedrijven en overheden, en bijgevolg ook de doeltreffendheid van publieke en private onlinediensten en elektronische handel in de interne markt van de Europese Unie te verhogen. De eIDAS-verordening regelt daartoe het grensoverschrijdend gebruik van elektronische identificatiemiddelen en vertrouwensdiensten tussen de lidstaten van de Europese Unie.
- 4.2.2 De eIDAS-verordening bevat een stelsel van erkenning van elektronische identificatiemiddelen (artikel 6 van de Verordening). Dat stelsel komt er in de kern op neer dat als een elektronisch identificatiemiddel is aangemeld bij de Europese Commissie en aan de door de Europese Commissie gestelde voorwaarden voldoet, alle Europese overheden die elektronische diensten aanbieden burgers de mogelijkheid moeten bieden om bij het gebruik van de betreffende diensten zich te identificeren aan de hand van het betreffende elektronische identificatiemiddel.
- 4.2.3 De eIDAS-verordening heeft uitsluitend betekenis voor de gemeente zodra een identificatiemiddel met succes is aangemeld bij de Europese Commissie. In een dergelijk

<sup>50</sup> Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (PbEU 2014, L 257).

<sup>51</sup> UITVOERINGSVERORDENING (EU) 2015/1502 VAN DE COMMISSIE van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt.



geval is de gemeente verplicht om bij het verlenen van haar elektronische diensten het mogelijk te maken dat gebruik kan worden gemaakt van het betreffende identificatiemiddel. Deze verplichting rust in een dergelijk geval echter op alle Europese overheden die elektronische diensten aanbieden. De verwachting is daarom dat op nationaal niveau invulling zal worden gegeven aan de verplichting tot het bieden van de mogelijkheid tot identificatie met een aangemeld elektronisch identificatiemiddel.

#### **4.3 Wet digitale overheid**

- 4.3.1 Aan de Tweede Kamer ligt momenteel het Wetsvoorstel Wet Digitale Overheid voor. In de huidige versie van het Wetsvoorstel is aan de Minister van Binnenlandse Zaken de bevoegdheid toegekend om bij ministeriële regeling betrouwbaarheidsniveaus voor te schrijven die bestuursorganen dienen te hanteren bij authenticatie in het kader van (bepaalde) elektronische overheidsdiensten:

Vgl. artikel 6 van het Wetsvoorstel Wet Digitale Overheid:

1. Bij elektronische dienstverlening waarvoor authenticatie op betrouwbaarheidsniveau substantieel of hoog vereist is, verlenen bestuursorganen en aangewezen organisaties uitsluitend toegang tot de dienstverlening indien gebruik wordt gemaakt van identificatiemiddelen die ten minste het voor de betreffende dienstverlening vereiste betrouwbaarheidsniveau hebben.
2. Bestuursorganen en aangewezen organisaties bepalen volgens bij ministeriële regeling te stellen regels voor welke door hen te verlenen elektronische diensten authenticatie op een bepaald betrouwbaarheidsniveau vereist is.

- 4.3.2 Net als de eIDAS-verordening bevat ook het Wetsvoorstel Wet Digitale Overheid een regeling voor de erkenning van identificatiemiddelen (maar dan op nationaal niveau). Artikel 9 van de Wet Digitale Overheid verplicht de Minister van Binnenlandse Zaken om onder de in dat artikel genoemde voorwaarden bepaalde private identificatiemiddelen "toe te laten". Zodra een identificatiemiddel is toegelaten, zijn alle bestuursorganen gehouden de mogelijkheid te bieden om in te loggen met dit identificatiemiddel.

Vgl. artikel 7 van de Wet Digitale Overheid:

Bestuursorganen accepteren bij hun elektronische dienstverlening aan natuurlijke personen waarvoor authenticatie op betrouwbaarheidsniveau substantieel of hoog vereist is, uitsluitend: a. alle toegelaten identificatiemiddelen, b. elektronische verklaringen als bedoeld in artikel 5, eerste lid, onderdeel b, en c. alle identificatiemiddelen die behoren tot een door een lidstaat van de Europese Unie ingevolge de eIDAS-verordening bij de Europese Commissie aangemeld en goedgekeurd stelsel.



Vgl. artikel 9, tweede lid, van de Wet Digitale Overheid:

Onze Minister kan, na het volgen van een door hem vast te stellen procedure, een privaat identificatiemiddel aanwijzen als toegelaten identificatiemiddel op het betrouwbaarheidsniveau substantieel of hoog, indien:

- a. dit noodzakelijk is voor de beschikbaarheid en toegankelijkheid van elektronische dienstverlening aan natuurlijke personen,
- b. het identificatiemiddel voldoet aan de in het eerste lid bedoelde technische specificaties en procedures, en
- c. de geschiktheid van dit identificatiemiddel is gebleken in een toets op basis van vooraf bekendgemaakte criteria.

3. Onze Minister is bevoegd tot het wijzigen, schorsen of intrekken van een toelating als bedoeld in het tweede lid.

4. Van een besluit op grond van het eerste, tweede of derde lid wordt mededeling gedaan door plaatsing in de Staatscourant waarbij het betrouwbaarheidsniveau van het betreffende identificatiemiddel wordt vermeld.

4.3.3 De Tweede en de Eerste Kamer hebben nog niet gestemd over het Westvoorstel Wet Digitale Overheid. Het is om die reden nog onzeker of de Wet Digitale Overheid er in zijn huidige vorm zal komen.

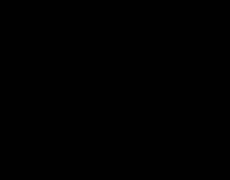
4.3.4 Daarbij komt dat op dit moment nog onzeker is of en, zo ja, op welke wijze de Minister van Binnenlandse Zaken gebruik zal maken van de bevoegdheid om betrouwbaarheidsniveaus voor te schrijven voor authenticatie bij digitale overheidsdiensten (artikel 6 Wetsvoorstel Wet Digitale Overheid). Ook is, voor zover wij weten, nog niet bekend welke procedure zal worden gehanteerd bij de toelating van authenticatiemiddelen (artikel 9 Wetsvoorstel Wet Digitale Overheid).

4.3.5 Dat neemt niet weg dat op zichzelf de Wet Digitale Overheid mogelijk wel voorwaarden zal gaan stellen aan het gebruik van authenticatiediensten zoals IRMA voor het gebruik van digitale overheidsdiensten. Onze verwachting is echter dat dergelijke voorwaarden nog niet op een termijn van twee jaar of korter van kracht zullen worden. Vooralsnog staat de Wet Digitale Overheid dus niet in de weg aan het gebruik van IRMA door de gemeente.

#### **4.4 Inschatting betrouwbaarheidsniveau IRMA**

4.4.1 De eIDAS-verordening onderscheidt drie betrouwbaarheidsniveaus: laag, substantieel en hoog, afhankelijk van de wijze waarop iemands identiteit wordt vastgesteld. In het Wetsvoorstel Wet Digitale Overheid is aangesloten bij deze betrouwbaarheidsniveaus.

Vgl. Artikel 8, tweede lid van de eIDAS-verordening:



De betrouwbaarheidsniveaus laag, substantieel en hoog voldoen respectievelijk aan de volgende criteria:

a) het betrouwbaarheidsniveau laag betreft een elektronisch identificatiemiddel in het kader van een stelsel voor elektronische identificatie, dat een beperkte mate van vertrouwen in iemands opgegeven of beweerde identiteit biedt, en wordt toegekend onder verwijzing naar technische specificaties, normen en procedures die daarmee verband houden, onder meer technische controles die tot doel hebben het risico van misbruik of wijziging van identiteit te verkleinen;


b) het betrouwbaarheidsniveau substantieel betreft een elektronisch identificatiemiddel in het kader van een stelsel voor elektronische identificatie, dat een substantiële mate van vertrouwen in iemands opgegeven of beweerde identiteit biedt, en wordt toegekend onder verwijzing naar technische specificaties, normen en procedures die daarmee verband houden, onder meer technische controles die tot doel hebben het risico van misbruik of wijziging van identiteit te verkleinen;

c) het betrouwbaarheidsniveau hoog betreft een elektronisch identificatiemiddel in het kader van een stelsel voor elektronische identificatie, dat een hogere mate van vertrouwen in iemands opgegeven of beweerde identiteit biedt dan een elektronisch identificatiemiddel met betrouwbaarheidsniveau substantieel, en wordt toegekend onder verwijzing naar technische specificaties, normen en procedures die daarmee verband houden, onder meer technische controles die tot doel hebben het risico van misbruik of wijziging van identiteit te voorkomen.

4.4.2 Zoals wij hiervoor concludeerden, is de betekenis van het betrouwbaarheidsniveau van IRMA op dit moment beperkt. Niettemin zou het betrouwbaarheidsniveau van IRMA in de toekomst vanwege het bepaalde in het Wetsvoorstel Wet Digitale Overheid wel van belang kunnen worden. Wij hebben daarom hierna, voor zover mogelijk, een inschatting gemaakt van het betrouwbaarheidsniveau van IRMA voor zover het gaat om de uitgifte en controle van door de gemeente uitgegeven BRP-gegevens. De betrouwbaarheidstoets is aldus beperkt tot het gebruik van IRMA voor de controle en uitgifte van gemeentelijke attributen, niet om IRMA als zodanig.

4.4.3 Voor het vaststellen van het betrouwbaarheidsniveau zijn de volgende elementen van belang:

a) de procedure om de identiteit van de natuurlijke of rechtspersoon die om uitgifte van het elektronisch identificatiemiddel verzoekt, te bewijzen en te verifiëren (artikel 8, derde lid, aanhef en onder a, eIDAS-verordening jo. paragraaf 2.1 van de bijlage bij de Uitvoeringsverordening EU 2015/1502);



b) de procedure voor de uitgifte van het aangevraagde elektronische identificatiemiddel (artikel 8, derde lid, b & f, eIDAS-verordening jo. paragraaf 2.2 van de Bijlage bij de Uitvoeringsverordening 2015/1502);

c) het authenticatiemechanisme, door middel waarvan de natuurlijke of rechtspersoon het elektronische identificatiemiddel gebruikt om zijn identiteit te bevestigen tegenover een vertrouwende partij;

d) de (kwaliteit van de)entiteit die het elektronische identificatiemiddel uitgeeft;

e) ieder ander orgaan dat betrokken is bij de uitgifte van het elektronische identificatiemiddel, en

f) de technische en veiligheidsspecificaties van het uitgegeven elektronische identificatiemiddel (artikel 8, derde lid, aanhef en onder c, eIDAS-verordening jo. paragraaf 2.3 van de Bijlage bij de Uitvoeringsverordening 2015/1502).<sup>52</sup>

4.4.4 Bovengenoemde elementen dienen los te worden beoordeeld. Het uiteindelijke betrouwbaarheidsniveau van het authenticatiemiddel wordt bepaald door het laagst scorende element.

4.4.5 Hieronder bespreken wij de afzonderlijke elementen en zullen wij, voor zover mogelijk, analyseren aan welk betrouwbaarheidsniveau IRMA voldoet. Wij merken daarbij op dat wij slechts een inschatting maken van het betrouwbaarheidsniveau van IRMA. Als met zekerheid zou moeten worden vastgesteld wat het betrouwbaarheidsniveau van IRMA is, zou dat een volledige analyse van IRMA en de Stichting vergen. Dat gaat de reikwijdte van dit advies te buiten.

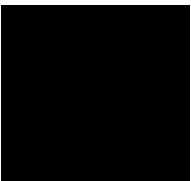
#### *Inschrijving*

4.4.6 De eisen die de eIDAS-verordening stelt aan de inschrijving is voor alle betrouwbaarheidsniveaus gelijk (zie paragraaf 2.1.1 van de Bijlage bij de Uitvoeringsverordening 2015/1502). De aanvrager (in geval van IRMA de gebruiker) moet bekend zijn met de voorwaarden die aan het gebruik van het identificatiemiddel zijn verbonden. Daarnaast moet de aanvrager bekend zijn met de aanbevolen veiligheidsvoorzorgen die aan het gebruik van het elektronische identificatiemiddel zijn verbonden. Tot slot moeten de relevante identificatiegegevens die voor het bewijs en de verificatie van de identiteit vereist zijn, zijn verzameld. IRMA voldoet in onze ogen aan de gestelde voorwaarden. De gebruiker wordt bij aanmelding afdoende geïnformeerd over IRMA als identificatiemiddel en over de wijze waarop de gebruiker veilig van IRMA gebruik kan maken.

<sup>52</sup> Vgl. Artikel 8 van de eIDAS-verordening, nader uitgewerkt in de Uitvoeringsverordening 2015/1502.

### *Bewijs en verificatie van de identiteit van de natuurlijke persoon*

- 4.4.7 Paragraaf 2.1.2 van de Bijlage bij de Uitvoeringsverordening stelt per betrouwbaarheidsniveau strenge eisen aan het bewijs en verificatie van de identiteit van de gebruiker. Het betrouwbaarheidsniveau is in belangrijke mate afhankelijk van de veiligheid van de identiteitsvaststelling van de natuurlijke persoon. De wijze van identiteitsvaststelling van gebruikers van IRMA en de manier waarop bij uitgevers attributen kunnen worden opgehaald is niet eenduidig. Zoals eerder toegelicht, hanteren uitgevers ten behoeve van IRMA afwijkende procedures voor het vaststellen van de identiteit van de gebruiker. Zo dient de gebruiker bij het ophalen van zijn BRP-gegevens bij de gemeente met DigiD in te loggen. In andere gevallen zal het opgeven van een naam en wachtwoord voldoende zijn (bijv. het ophalen van social netwerk-attributen). Dit betreft in vergelijking met DigiD een minder betrouwbare manier van het vaststellen van de identiteit van de betrokkene.
- 4.4.8 Worden de afzonderlijke methoden aan de hand van paragraaf 2.1.2 van de Bijlage bij de Uitvoeringsverordening beoordeeld, dan leidt dit ertoe dat er bij het bewijs en de verificatie van de identiteit van de gebruiker per uitgever afwijkende beveiligingsniveaus bestaan, afhankelijk van de door de gebruiker gekozen verificatiemethode:
- de door de gemeente gehanteerde inlogmethode (DigiD met sms) voor de uitgifte van attributen heeft betrouwbaarheidsniveau laag. Op dit moment wordt gebruikgemaakt van DigiD-midden, oftewel het inloggen met een DigiD gebruikersnaam en wachtwoord in combinatie met een sms-code. De sms-code wordt verstuurd naar de geregistreerde mobiele telefoon van de gebruiker. Deze DigiD inlogmethode wordt op grond van de eIDAS-verordening aangemerkt als betrouwbaarheidsniveau laag. Dit straalt af op het totale betrouwbaarheidsniveau van IRMA voor zover het gaat om gemeentelijke credentials. Doordat het uiteindelijke betrouwbaarheidsniveau van het gebruik van IRMA wordt bepaald door de laagste score, heeft dit automatisch tot gevolg dat het gebruik van IRMA door de gemeente niet hoger kan komen dan betrouwbaarheidsniveau laag. Dit kan op de korte termijn veranderen. Het zal voor burgers mogelijk worden om middels de DigiD-app gebruik te maken van DigiD Substantieel. Bij DigiD Substantieel wordt de betrouwbaarheid van de verificatie van de identiteit van de burger verhoogd doordat de app wordt gekoppeld aan het paspoort, de rijbewijs of de identiteitskaart van de burger. Het is vooralsnog niet voor alle burgers mogelijk om het betrouwbaarheidsniveau van hun DigiD op te schalen naar substantieel. Dit heeft te maken met de omstandigheid dat het scannen van de chip in het paspoort, de rijbewijs of de identiteitskaart slechts kan plaatsvinden door middel van Android telefoons. Met een iPhone is het (vooralsnog althans) niet mogelijk om de app te koppelen aan de identiteitskaart van de gebruiker. Wordt dit in de toekomst wél mogelijk, dan kan de gemeente het betrouwbaarheidsniveau van het gebruik van IRMA (voor dit onderdeel van de betrouwbaarheidstoets) kunnen verhogen



naar substantieel door elke gebruiker van IRMA te verplichten tot het gebruik van DigiD Substantieel. Daar is vooralsnog geen sprake van.<sup>53</sup>

Bij andere attributen dan gemeentelijke attributen kunnen, afhankelijk van de gekozen verificatiemethoden, andere betrouwbaarheidsniveaus gelden:

- De sociale netwerk-attributen, het e-mail attribuut, het mobiele telefoon-attribuut en de attributen afkomstig van (Nederlandse) onderwijsinstellingen hanteren allemaal een inlogmethode die kwalificeert als betrouwbaarheidsniveau laag.
- Tot slot is het mogelijk om via iDeal en iDIN onder meer de IBAN en BIC op te halen. IDIN hanteert het betrouwbaarheidsniveau substantieel.

#### *Het beheer van elektronische identificatiemiddelen*

- 4.4.9 Paragraaf 2.2.1 van de Bijlage bij de Uitvoeringverordening stelt eisen aan de kenmerken en het ontwerp van elektronische identificatiemiddelen. Onze inschatting is dat de kenmerken van het ontwerp van IRMA in ieder geval voldoen aan betrouwbaarheidsniveau substantieel en mogelijk zelfs hoog. IMRA maakt gebruik van ten minste twee authenticatiefactoren die tot verschillende categorieën behoren. IRMA is zodanig ontworpen dat het kan worden verondersteld slechts te worden gebruikt door of onder controle van de persoon aan wie het toebehoort. IRMA biedt zoals reeds toegelicht bescherming tegen kopiëring en vervalsing en tegen aanvallers met een hoog aanvalspotentieel. IRMA is zodanig ontworpen dat het door de persoon aan wie de identiteit toebehoort op betrouwbare wijze kan worden beschermd tegen gebruik door anderen.


#### *De uitgifte, uitreiking en activering*

- 4.4.10 Wij achten het verdedigbaar dat de wijze van uitgifte, uitreiking en activering van het als betrouwbaarheidsniveau substantieel kwalificeert. De uitgifte van het IRMA-account en het ophalen van de attributen vindt plaats via een verificatiemechanisme waarmee kan worden verondersteld dat alleen de persoon aan wie het toebehoort in het bezit ervan wordt gesteld. (zie paragraaf 2.2.2. van de Bijlage bij de Uitvoeringsverordening).

#### *Schorsing, herroeping en reactivering*

- 4.4.11 Voor het betrouwbaarheidsniveau voor schorsing, herroeping en reactivering gelden voor alle betrouwbaarheidsniveaus dezelfde vereisten. Voor zover wij kunnen overzien, voldoet IRMA hieraan. Het is mogelijk het IRMA-account snel en doeltreffend te schorsen. Er bestaan

<sup>53</sup> Dit betrouwbaarheidsniveau zal enkel gelden voor de credentials die door de gemeente zijn uitgegeven. De credentials die door andere uitgevers via IRMA worden uitgegeven zullen, zoals wij hierna zullen toelichten, mogelijk onder een ander betrouwbaarheidsniveau vallen.



bovendien maatregelen om ongeoorloofde schorsing, herroeping en reactivering te voorkomen.

#### *Verlening en vervanging*

- 4.4.12 Het betrouwbaarheidsniveau voor verlening en vervanging kan worden ingeschat als substantieel (paragraaf 2.2.4). Dit vereiste bepaalt dat rekening houdend met het risico dat de persoonsidentificatiegegevens zijn gewijzigd, voor verlenging of vervanging aan dezelfde betrouwbaarheidsvereisten moet zijn voldaan als voor het initiële proces van bewijs en verificatie van de identiteit, of moet worden uitgegaan van een geldig elektronisch identificatiemiddel met hetzelfde of een hoger betrouwbaarheidsniveau. IRMA biedt deze mogelijkheid nu attributen na verloop van tijd verlopen en moeten worden vervangen. Het betrouwbaarheidsniveau is daarmee substantieel.

#### *Authenticatiemechanisme*

- 4.4.13 Wij achten het betrouwbaarheidsniveau voor de door IRMA gehanteerde authenticatiemechanisme op zijn minst substantieel en mogelijk zelfs hoog (paragraaf 2.3.1 van de Bijlage). De door IRMA gehanteerde cryptografie en keyshare server maken het mogelijk dat de geldigheid van de persoonsidentificatiegegevens op een betrouwbare wijze worden geverifieerd door middel van dynamische authenticatie. Bovendien voorziet IRMA in beveiligingscontroles ter verificatie van de identiteit van de gebruiker die het zeer onwaarschijnlijk maken dat de authenticatiemechanismen kunnen worden omzeild door methoden als gissen, afluisteren, herafspelen of manipuleren van communicatie door een aanvaller met een gematigd aanvalspotentieel.


#### *Beheer en organisatie*

- 4.4.14 Tot slot dient IRMA te voldoen aan vereisten die worden gesteld aan het beheer en de organisatie van het identificatiemiddel. IRMA dient kortgezegd te beschikken over gedocumenteerde methoden en beleid voor het beheer van informatiebeveiliging, benaderingen voor risicobeheersing en andere erkende controlemethoden, zodat garanties kunnen worden geboden dat in doeltreffende praktijken is voorzien. Ervan uitgaande dat periodieke audits en technische controles worden uitgevoerd door de Stichting achten wij het betrouwbaarheidsniveau van IRMA op het gebied van beheer en organisatie substantieel.

#### **Conclusie**

- 4.4.15 Op basis van het voorgaande is onze inschatting dat het betrouwbaarheidsniveau van IRMA als overwegend substantieel moet worden beschouwd, zij het dat de inlogmethode om attributen te verkrijgen (iDEAL met sms-verificatie) op dit moment als betrouwbaarheidsniveau 'laag' moet worden aangemerkt. Wij schatten aldus in dat het gebruik van IRMA door de gemeente onder de eIDAS-verordening zal worden aangemerkt





als een identificatiemiddel met betrouwbaarheidsniveau 'laag'. Dit zal binnenkort anders kunnen komen te liggen op het moment dat Digid-substantieel landelijk voor alle burgers beschikbaar wordt. Vanaf dat moment zou het gebruik van IRMA door de gemeente het betrouwbaarheidsniveau 'substantieel' kunnen verkrijgen.