PELS RIJCKEN

Juridisch kader voor Regie op gegevens

Sandra van Heukelom-Verhage en Nina Bontje
24 januari 2020

Inhoud

1 Inleiding

Momenteel bestaan en ontstaan er verschillende sectorale afsprakenstelsels en andere regietoepassingen om burgers te ondersteunen bij het voeren van regie op hun gegevens. Een kader voor regie op gegevens moet mogelijk maken dat zo verantwoord mogelijk vorm kan worden gegeven aan nieuwe mogelijkheden voor regie op gegevens, zonder de innovatie op zichzelf te frustreren. Het kader biedt daartoe een aantal basisafspraken en ontwerpprincipes.

In dit stuk staat het *juridisch* kader voor regie op gegevens centraal, dat onderdeel uitmaakt van het bredere kader voor regie op gegevens.

Het juridisch kader wordt gevormd door wettelijke regelingen en afspraken/spelregels. Het doel van dit juridisch kader is tweeledig:

1. Het bieden van een overzicht van wettelijke regels die in de regel van toepassing zullen zijn bij regie op gegevens; en
2. Het bieden van inzicht in de juridische onderbouwing voor afspraken/spelregels die moeten worden gemaakt bij een kader voor regie op gegevens.

Niet voor alle afspraken/spelregels die in het kader terugkomen, is een juridische onderbouwing terug te vinden in wet- en regelgeving. Sommige afspraken/spelregels zijn gebaseerd op waarden die niet wettelijk zijn verankerd. Dat roept de vraag op of die waarden alsnog een juridische basis moeten krijgen. Dat hoeft niet altijd; in sommige gevallen kunnen waarden op zichzelf bestaan, terwijl in andere gevallen een wettelijke basis gewenst is. In dit juridisch kader ligt de focus evenwel op bestaande wet- en regelgeving en daaruit voortvloeiende afspraken/spelregels.

Leeswijzer

Het juridisch kader is als volgt opgebouwd:

- In hoofdstuk 2 worden een aantal relevante begrippen toegelicht;
- In hoofdstuk 3 wordt nader ingegaan op hoe wettelijke regelingen zich verhouden tot afspraken die moeten worden gemaakt bij sectorale afsprakenstelsels en andere regie toepassingen;
- In hoofdstuk 4 wordt generieke wet- en regelgeving besproken die vaak van toepassing zal zijn op sectorale afsprakenstelsels en andere regietoepassingen;
- In hoofdstuk 5 worden de aanvullende juridische spelregels/afspraken besproken.

2 Begrippen

Regiehandelingen
De wettelijke regelingen en afspraken hebben betrekking op vijf functies (handelingen) in het proces van het voeren van regie op gegevens, te weten:

- verzamelen;
- inzage;
- correctie;
- toestemming voor gebruik;
- gebruik; en
- beëindigen van toestemming.

Persoonsgegevens en (andere) gegevens
Met gegevens wordt zowel gedoeld op persoonsgegevens als op alle andere gegevens waarop regie kan worden gevoerd.

Persoonsgegevens is een term afkomstig uit de Algemene Verordening Gegevensbescherming (AVG) en betreft, kort gezegd, alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Het gaat dan zowel om direct identificeerbare informatie (zoals een naam, identificatienummer of foto) als om indirect identificeerbare informatie (zoals locatiegegevens).

Regie op gegevens gaat over meer dan alleen persoonsgegevens. Gegevens over bedrijven of organisaties zullen in veel gevallen niet herleidbaar zijn tot natuurlijke personen en dan dus geen persoonsgegevens zijn. Voorts ziet het persoonsgegevensbegrip alleen op de gegevens over een persoon als zodanig, en niet ook op de drager van die gegevens, zoals een document, of op een geattesteerde bewering. Een afnemer – dat is: degene die gegevens nodig heeft voor (bijvoorbeeld) het leveren van een dienst – zal vaak niet of niet alleen over persoonsgegevens willen beschikken om een dienst te leveren, maar ook zeker willen zijn dat een bepaalde bewering over de burger waar is, bijvoorbeeld door verkrijging van een gewaarmerkt document of door attestatie van een bewering. Daarvoor zijn andere gegevens dan (alleen) persoonsgegevens nodig, zoals documenten of geattesteerde beweringen.

> Als voorbeeld kan een diploma worden genomen, waarop staat dat burger X met geboortedatum Y een masterdiploma in Z heeft behaald. Men zou op drie lagen regie kunnen voeren, te weten:
>
> • De verschillende (persoons)gegevens in het document: de naam, geboortedatum en het gegeven dat burger X een masterdiploma in Z heeft behaald;
> • De geverifieerde/geattesteerde bewering dat burger X master Z heeft afgerond. Er zijn situaties denkbaar waarin een afnemer niet zozeer persoonsgegevens wil ontvangen om een dienst te leveren, maar er alleen

zeker van wil zijn dat de (verder anonieme) burger is afgestudeerd in een bepaalde richting; of
• Het diploma (het document) of een kopie daarvan als drager van de informatie dat burger X is afgestudeerd.

Uitgangspunt is dan ook dat regiehandelingen in de regel zien op verschillende soorten gegevens, waaronder persoonsgegevens, maar niet alleen op persoonsgegevens. Deze andere, aanvullende gegevens worden – samen met persoonsgegevens – aangeduid als gegevens.

Actoren
In dit juridisch kader wordt steeds gedoeld op de wettelijke regelingen en afspraken die van toepassing zijn op de verschillende actoren in het proces van het voeren van regie op gegevens. Het gaat dan om:

- de aanbieder: degene die gegevens aanbiedt;
- de afnemer: degene die gegevens nodig heeft voor (bijvoorbeeld) het leveren van een dienst;
- de burger;
- en eventuele andere partijen, zoals verwerkers en platformaanbieders.

Toepassingsbereik: sectorale afsprakenstelsels en andere regietoepassingen
Er ontstaan op dit moment verschillende afsprakenstelsels en concrete regietoepassingen om burgers te ondersteunen bij het hebben van regie op hun gegevens. Daarbij kan worden gedacht aan MedMij in het zorgdomein, EduMij in het onderwijsdomein en MaaS in het vervoersdomein. Dit juridisch kader biedt afspraken/spelregels waar dergelijke sectorale afsprakenstelsels en regietoepassingen rekening mee moeten houden.

3 De wettelijke regulering van afsprakenstelsels en regietoepassingen

3.1 Inleiding: de juridisch te onderscheiden afsprakenstelsels en regietoepassingen

Gelet op de verscheidenheid van afsprakenstelsels en regietoepassingen kan niet op voorhand één sluitend juridisch kader worden voorgeschreven. Allereerst moet onderscheid worden gemaakt tussen generieke wet- en regelgeving, die op veel afsprakenstelsels en regietoepassingen van toepassing zal zijn, en sectorspecifieke wet- en regelgeving, die op bepaalde afsprakenstelsels en regietoepassingen van toepassing zal zijn. Daarnaast zullen er afsprakenstelsels en regietoepassingen zijn die al in grote mate wettelijk zijn gereguleerd en afsprakenstelsels en regietoepassingen die dat niet of nauwelijks zijn. Er zal (en moet) als gevolg daarvan – per geval – worden vastgesteld welk specifieke juridisch kader van toepassing is.

Om dat te bepalen, zijn de volgende vragen van belang:

- Is de *dienst* die binnen het afsprakenstelsel of de regietoepassing wordt geleverd wettelijk gereguleerd?
- Bestaat er specifieke wet- en regelgeving over de *gegevens* die vloeien ten behoeve van de te leveren dienst?

Als wordt uitgegaan van deze vragen, dan kunnen de volgende uitgangssituaties worden onderscheiden:

1. Wettelijk gereguleerde diensten met bepalingen over de verwerking van gegevens

In deze situaties zijn de diensten én de in dat kader te verwerken gegevens wettelijk geregeld.

Voorbeeld: de regietoepassing van de rekenhulp voor de Wet maatschappelijke ondersteuning 2015 (Wmo). Het Centraal administratiekantoor (CAK) heeft de wettelijke taak de hoogte van de eigen bijdrage in de zorg te controleren (artikel 2.1.4 Wmo). De dienst van het CAK is daarmee wettelijke geregeld. In de Wmo is voorts geregeld dat het CAK daarvoor gebruikmaakt van inkomensgegevens van de Belastingdienst (artikel 5.1.3 en 5.2.3 Wmo). Daarmee ligt op voorhand vast dat de Belastingdienst in bepaalde situaties inkomensgegevens aan het CAK moet verstrekken onder de daarvoor voorgeschreven voorwaarden.

2. Wettelijk gereguleerde diensten zonder bepalingen over de verwerking van gegevens

In deze situatie is de dienst wel wettelijk geregeld, maar bestaan er geen wettelijke bepalingen over de ten behoeve daarvan te verwerken gegevens.

Voorbeeld: de regietoepassing 'verkenning e-inkomenstoets'. Woningcorporaties zijn wettelijk verplicht bij de verhuur van een woning een inkomenstoets uit te voeren. Niet geregeld is op basis van welke gegevens woningcorporaties die toets uitvoeren. In de praktijk maken woningcorporaties gebruik van door de (potentiële) huurder aangeleverde inkomensgegevens. De Belastingdienst verstrekt deze gegevens aan de huurder. In deze situatie is de dienst (de inkomenstoets) wettelijk geregeld, maar de verwerking van gegevens niet.

3. Niet wettelijk gereguleerde diensten en geen bepalingen over de verwerking van gegevens

Dit zijn situaties waarin de markt voor onverplichte diensten afsprakenstelsels of regietoepassingen ontwikkelt.

Voorbeeld: een regietoepassing voor het aankopen van een huis.

4. Systemen voor verschillende gegevensuitwisselingen

Dit zijn situaties waarin systemen voor gegevensuitwisselingen worden ontwikkeld met regie door de burger als opzichzelfstaand doel (en niet zozeer een concrete toepassing).

Voorbeeld: MedMij.

5. Rechtstreekse wettelijke relaties

Dit zijn situaties die in feite buiten dit kader vallen, omdat deze betrekking hebben op een rechtstreekse relatie tussen de burger en één partij. Die partij is de dienstverlener en kan, naast de burger, ook aanbieder van gegevens zijn.

Voorbeeld: het toekennen van toeslagen door de Belastingdienst.

3.2 De mate van wettelijke regulering en de gevolgen voor regie

In gevallen waarin afsprakenstelsels en regietoepassingen al in vergaande mate wettelijk zijn gereguleerd, moeten deze afsprakenstelsel en regietoepassingen steeds aansluiten bij die wettelijke regeling of regelingen. De aanwezige ruimte voor het voeren van regieactiviteiten is afhankelijk van de ruimte die de wet biedt. Daar waar afsprakenstelsels en regietoepassingen niet of nauwelijks wettelijk zijn gereguleerd, zal meer vrijheid zijn voor de wijze waarop een burger de regie kan worden gegeven over zijn of haar gegevens.

3.3 De mate van wettelijke regulering en het belang van afspraken/spelregels

De mate van wettelijke regulering heeft voorts gevolgen voor de mate waarin aanvullende waarborgen moeten worden getroffen voor de burger. Als gegevens stromen op grond van specifieke wettelijke regelingen, dan gaat dat veelal gepaard met de nodige waarborgen die al in die wettelijke regelingen zijn neergelegd. Denk daarbij aan bepalingen over doelbinding en proportionaliteit.

Bij regietoepassingen waarbij de gegevensstromen niet of in mindere mate wettelijk zijn gereguleerd, ontbreekt een dergelijk gesloten ecosysteem met concrete waarborgen. In die situaties is de behoefte aan afspraken/spelregels dan ook groter dan in de situaties waar de waarborgen al in de wet zijn gereguleerd.

3.4 Deelconclusie

Ieder sectoraal afsprakenstelsel of regietoepassing kan worden geplaatst in een van de bovengenoemde categorieën. Op basis daarvan kan vervolgens worden vastgesteld:

1. of, en zo ja op welke wijze er ruimte bestaat voor het uitoefenen van regieactiviteiten; en
2. welke afspraken er moeten worden gemaakt om de leemten te vullen ten aanzien van waarborgen voor de burger, zoals doelbinding en proportionaliteit.

De te maken afspraken/op te stellen spelregels bespreken wij in hoofdstuk 5. Voorafgaand daaraan wordt in hoofdstuk 4 eerst de generieke wet- en regelgeving besproken die vaak van toepassing zal zijn op sectorale afsprakenstelsels en regietoepassingen.

4 Generieke wet- en regelgeving

4.1 Inleiding

In dit hoofdstuk bespreken wij generieke wet- en regelgeving die in veel gevallen (in ieder geval) van toepassing zal zijn op sectorale afsprakenstelsels en regietoepassingen.

Deze bespreking is niet uitputtend bedoeld. Steeds zal, per geval, moeten worden nagegaan of 1) deze generieke wet- en regelgeving daadwerkelijk van toepassing is en 2) of er aanvullende wet- en regelgeving van toepassing is.

Wetsvoorstellen, verordeningen en richtlijnen die nog niet in werking zijn getreden, zijn buiten beschouwing gelaten.

4.2 Eigendom van data?

Bij regie op gegevens gaat het om het vergroten van de zeggenschap van de burger over 'zijn gegevens'. Bij de ontwikkeling van afsprakenstelsels rijst vrijwel steeds de vraag van wie de gegevens vanuit juridisch perspectief zijn. Burgers zijn veelal van mening dat persoonsgegevens van hun zijn, omdat ze over hen gaan. Afnemers en aanbieders denken daar vaak anders over, zeker als zij veel moeite hebben moeten doen om die gegevens te verzamelen en te ordenen. Zij zien die gegevens dan als onderdeel van hun bedrijfsvoering. Eigenlijk is deze discussie terug te voeren op de vraag wie het eigendom heeft van gegevens of data. Hier wringt de schoen, omdat het Nederlandse rechtsstelsel geen bepaling kent over het eigendom van gegevens en data. Het eigendomsbegrip in het Burgerlijk wetboek is alleen van toepassing op stoffelijke zaken, en dat zijn gegevens en data niet. Daarom kan geen eenduidig en expliciet antwoord worden gegeven op de vraag van wie gegevens en data zijn. Er zal daarom te raden moeten worden gegaan bij minder expliciete wetgeving, bijvoorbeeld wetgeving die ingaat op de vraag wie rechthebbende is op de gegevens of data of wie aanspraak kan maken op de datadrager. Dat maakt de discussie en de uitkomst soms wat diffuus. Belangrijker voor dit juridisch kader is evenwel dat gegevens veilig en betrouwbaar, met regie van de burger, kunnen worden verwerkt. Daarvoor zijn vooral de hierna te bespreken waarborgen, rechten en plichten van belang.

4.3 Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG)

Inleiding

Bij sectorale afsprakenstelsels en andere regietoepassingen zullen vaak (ook) persoonsgegevens worden verwerkt. Bij de verwerking van persoonsgegevens is de AVG leidend.[1]

> **Persoonsgegevens** zijn: "alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon" (zie artikel 4, aanhef en onder 1, AVG).
>
> **Verwerking** is: "een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens" (artikel 4, aanhef en onder 2, AVG).
>
> Gegevens over een bedrijf zijn, als deze niet herleidbaar zijn tot een identificeerbaar persoon, geen persoonsgegevens. Op de verwerking van bedrijfsgegevens is de AVG dan ook niet van toepassing. Zie daarover ook het in hoofdstuk 2 gemaakte onderscheid tussen persoonsgegevens en andere gegevens.

De AVG biedt zowel kaders waarover moet worden nagedacht bij de verwerking van persoonsgegevens als materiële eisen waaraan (in ieder geval) moet worden voldaan. Waar nodig zijn deze regels uitgewerkt in de Nederlandse UAVG.

Actoren en de AVG

De verschillende actoren moeten bij regie op persoonsgegevens steeds worden gekwalificeerd op basis van de verschillende actoren die de AVG kent. Het gaat daarbij doorgaans om de verwerkingsverantwoordelijke en de (sub)verwerker. De afnemer en de aanbieder zullen in de regel als verwerkingsverantwoordelijken kwalificeren.

De verwerkingsverantwoordelijke speelt in het stelsel van de AVG een centrale rol. Een verwerkingsverantwoordelijke is degene die, alleen of samen met anderen, het

[1] Naast eventuele bijzondere gegevensbeschermingsregelingen die van toepassing kunnen zijn, zoals in de Wet op de geneeskundige behandelovereenkomst (WGBO).

doel en de middelen van de verwerking van persoonsgegevens vaststelt (artikel 4, aanhef en onder 7, AVG).

> Met het bepalen van het doel van de verwerking wordt bedoeld dat de verwerkingsverantwoordelijke de zeggenschap heeft over waarom de persoonsgegevens worden verwerkt en voor welke concrete doelen de persoonsgegevens zullen worden ingezet. Het vaststellen van het doel van de verwerking is een exclusieve bevoegdheid van de verwerkingsverantwoordelijke.
>
> Met het vaststellen van de middelen van de verwerking wordt gedoeld op het vaststellen van de wijze waarop de verwerking plaats zal vinden, kortom: hoe worden de persoonsgegevens verwerkt ten behoeve van het vastgestelde doel.

Indien twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en de middelen van de verwerking bepalen, wordt gesproken van 'gezamenlijke verwerkingsverantwoordelijken'. Zij zijn verplicht een zogenoemde onderlinge regeling vat te stellen, waarin zij hun respectievelijke verantwoordelijkheden ten aanzien van de naleving van de AVG vastleggen (artikel 26, eerste lid, AVG).

Een eventuele identiteitsaanbieder en/of identiteitsmakelaar of een platformaanbieder zal veelal kwalificeren als verwerker van de aanbieder en/of afnemer. De verwerker is degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt (artikel 4, aanhef en onder 8, AVG). Kenmerkend voor een verwerker is dat de verwerker:

- een externe natuurlijke persoon, rechtspersoon, overheidsinstantie, dienst of orgaan is, die geen onderdeel vormt van de verwerkingsverantwoordelijke, en;
- persoonsgegevens voor de verwerkingsverantwoordelijke verwerkt – en dus niet voor zichzelf.

Voor de kwalificatie van verwerker is bepalend of de partij aanwijzingen van de verwerkingsverantwoordelijke dient op te volgen met betrekking tot de verwerking van persoonsgegevens. Zo ja, dan is de partij een verwerker.

De verwerker ontleent zijn bevoegdheid om persoonsgegevens te verwerken aan de bevoegdheid van de verwerkingsverantwoordelijke die hem inschakelt. De bevoegdheden van een verwerker moeten zijn vastgelegd in een verwerkersovereenkomst (artikel 28, derde lid, AVG).

Voor de vraag of een actor kwalificeert als verwerkingsverantwoordelijke of verwerker is ook relevant het 'Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker"' van de Groep gegevensbescherming artikel 29.

Daarin gaat de Groep gegevensbescherming artikel 29 onder meer ook in op de vraag hoe clouddiensten kwalificeren.

Regieactiviteiten en de AVG

Voor de regieactiviteiten *inzage*, *correctie* en *gebruik* zijn de rechten van de betrokkene – dat is: degene op wie persoonsgegevens betrekking hebben –[2] uit de AVG relevant.

Een persoon kan zijn persoonsgegevens *inzien* door een inzageverzoek op grond van artikel 15 AVG te doen bij de aanbieder of afnemer. Het inzagerecht van de AVG beperkt zich tot een recht voor een betrokkene om inzage te krijgen in de hem betreffende persoonsgegevens die door een verwerkingsverantwoordelijke worden verwerkt, en omvat niet ook een recht op de documenten/dragers van die persoonsgegevens of op geattesteerde beweringen (artikel 15, eerste en tweede lid, AVG).

Naast het bieden van inzage in de verwerkte persoonsgegevens zal een verwerkingsverantwoordelijke de betrokkene moeten informeren over onder meer de verwerkingsdoeleinden, de categorieën van persoonsgegevens en de (categorieën van) ontvangers (artikel 15, tweede lid, AVG).

Verder hebben betrokkenen recht op een kopie van de persoonsgegevens die worden verwerkt (artikel 15, derde lid, AVG). Bij de honorering van een inzageverzoek kan een kopie worden verstrekt van het document dat de drager die de persoonsgegevens bevat (al dan niet met weglakking van de informatie die geen persoonsgegevens bevat). Er kan echter ook een overzicht worden verstrekt dat een kopie van de persoonsgegevens bevat (zie daarover ook de website van de Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/gebruik-uw-privacyrechten/recht-op-inzage).

Overigens kan inzage door een aanbieder of afnemer worden beperkt of geweigerd in geval een uitzonderingsgrond van artikel 23 AVG jo. artikel 41 Uitvoeringswet AVG zich voordoet, zoals het waarborgen van een taak op het gebied van toezicht.

Het structureel en/of op grote schaal verstrekken van persoonsgegevens door een aanbieder aan of via een betrokkene ten behoeve van regie op gegevens middels het inzagerecht van de AVG, lijkt oneigenlijk gebruik van dit recht. Daarvoor zal veelal een stevigere en specifiekere wettelijke basis nodig zijn.

Volledigheidshalve wordt opgemerkt dat sommige domeinen "eigen" inzageregelingen kennen, die zijn opgenomen in bijzondere wetten. Zie bijvoorbeeld de bepalingen in Boek 7 van het Burgerlijk Wetboek inzake de geneeskundige behandeling. Op grond

[2] Bij de bespreking van de AVG gaan wij uit van het begrip "betrokkene', conform het bepaalde in artikel 4, aanhef en onder 1, AVG.

van artikel 7:456 BW moet een hulpverlener een patiënt in beginsel desgevraagd inzage geven in en een afschrift geven van de bescheiden in een patiëntendossier.

Voor het *corrigeren* van persoonsgegevens kan een persoon een rectificatieverzoek bij een verwerkingsverantwoordelijke indienen (zie artikel 16 AVG). Ook dat recht kan op grond van artikel 23 AVG jo. artikel 41 Uitvoeringswet AVG worden beperkt of geweigerd.

De AVG heeft als doel de verwerking van persoonsgegevens zodanig te reguleren, dat er geen belemmering meer hoeft te zijn voor het vrije verkeer van persoonsgegevens. Voor het *delen* (*gebruiken*) van persoonsgegevens kent de AVG het recht op overdraagbaarheid van persoonsgegevens (artikel 20 AVG), dat ook wel het recht op dataportabiliteit wordt genoemd. Door gebruikmaking van dit recht kan een persoon zijn persoonsgegevens (die de betrokkene vaak zelf heeft aangeleverd, zoals contactgegevens in een mobiele telefoon) doorgeven van de ene dienstverlener aan een andere dienstverlener. Dat recht kan alleen worden ingeroepen bij verwerkingen van persoonsgegevens die berusten op toestemming of een overeenkomst (zie artikel 6, eerste lid, aanhef en onder a en b, AVG) en als die verwerkingen via automatische procedures worden verricht. Ook dit recht kan worden beperkt of geweigerd en is ongeschikt voor het structureel en/of op grote schaal verstrekken van persoonsgegevens door een aanbieder en/ of afnemer aan of via een persoon ten behoeve van regie op gegevens.

Waarborgen in de AVG

De AVG bevat waarborgen voor het verwerken van persoonsgegevens. Er bestaat bij de verwerking van persoonsgegevens, zo is het uitgangspunt, voor de aanbieder een grondslag om die persoonsgegevens te verstrekken aan de afnemer en voor de afnemer een grondslag om die persoonsgegevens vervolgens te verwerken. Dat kan zowel een specifieke grondslag zijn in een bijzondere wet, als een algemene grondslag van de AVG. De algemene grondslagen van de AVG zijn terug te vinden in artikel 6 AVG en betreffen (kort gezegd):

a) De ondubbelzinnige toestemming. Deze toestemming moet een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting betreffen;
b) De uitvoering of totstandkoming van een overeenkomst;
c) De wettelijke verplichting;
d) De vrijwaring van een vitaal belang van de betrokkene;
e) De goede vervulling van een taak van algemeen belang/uitoefening van het openbaar gezag; en
f) Een gerechtvaardigd belang van de verwerkingsverantwoordelijke of een derde.

Die grondslagen gaan steeds gepaard met waarborgen voor de persoon, die – in de regel – rusten op de aanbieder en de afnemer als verwerkingsverantwoordelijken. Zo mogen persoonsgegevens alleen worden verzameld voor specifieke, gerechtvaardigde

doeleinden en mogen persoonsgegevens niet zonder toestemming verder worden verwerkt op een met die doeleinden onverenigbare wijze (het beginsel van doelbinding). Daarnaast moeten de persoonsgegevens toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (het beginsel van dataminimalisatie). Verder moeten de persoonsgegevens juist zijn en zo nodig worden geactualiseerd (het beginsel van juistheid), niet langer worden bewaard dan noodzakelijk (het beginsel van opslagbeperking) en goed worden beveiligd (het beginsel van integriteit en vertrouwelijkheid) (zie artikel 5, eerste lid, AVG voor de beginselen inzake de verwerking van persoonsgegevens).

Voor gevoelige persoonsgegevens, te weten: bijzondere persoonsgegevens, strafrechtelijke persoonsgegevens en nationale identificatienummers, zoals het BSN, geldt een verzwaard regime. Verwerking van bijzondere persoonsgegevens is in beginsel verboden, tenzij er een uitzondering van toepassing is (artikel 9 AVG jo. artikel 22 tot en met 30 UAVG). Ook voor de verwerking van strafrechtelijke persoonsgegevens zal steeds een grond moeten bestaan (artikel 10 AVG jo. artikel 31 tot en met 33 UAVG). Daarnaast mag een nationaal identificatienummer, zoals het BSN, pas worden verwerkt als de wet daarvoor een grondslag biedt (artikel 87 AVG jo. artikel 46 UAVG).

Ook rust op de verwerkingsverantwoordelijken de verplichting om betrokkenen te informeren over de verwerkingen van persoonsgegevens die bij de regietoepassing plaatsvinden (artikel 13 en 14 AVG). Meer concreet dient iedere verwerkingsverantwoordelijke op grond van artikel 13 AVG de betrokkene te informeren over:

- diens identiteit en contactgegevens en, indien aan de orde, die van zijn vertegenwoordiger;
- in voorkomend geval, de contactgegevens van de functionaris gegevensbescherming;
- de doelen waarvoor de persoonsgegevens worden verwerkt en de rechtsgrond van de verwerking;
- (indien aan de orde) het gerechtvaardigd belang waarop de verwerking is gebaseerd;
- de (categorieën van) ontvangers;
- eventuele doorgiften van persoonsgegevens aan een derde land of een internationale organisatie en aanvullende informatie hierover;
- de bewaartermijn van de persoonsgegevens of, als dat niet mogelijk is, de criteria ter bepaling van die termijn;
- de rechten van de betrokkene;
- of de verstrekking van persoonsgegevens een wettelijke of contractuele verplichting is, dan wel een noodzakelijke voorwaarde is om een overeenkomst te sluiten, en of de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer deze gegevens niet worden verstrekt;
- als de verwerking op toestemming is gebaseerd: 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
• (voor zover aan de orde) het bestaan van geautomatiseerde besluitvorming bij de regietoepassing en nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

Als de persoonsgegevens niet van de betrokkene zelf zijn verkregen, moet de verwerkingsverantwoordelijke de betrokkene ook informeren over:

• de betrokken categorieën van persoonsgegevens; en
• de bron waar de persoonsgegevens vandaan komen, en in voorkomend geval, of zij afkomstig zijn van openbare bronnen.

Op grond van artikel 12 AVG moet de verwerkingsverantwoordelijke passende maatregelen nemen opdat de betrokkene bovenstaande informatie in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm verkrijgt en in duidelijke en eenvoudige taal. In de praktijk wordt de informatie vaak gegeven door middel van een schriftelijke privacyverklaring die fysiek of elektronisch aan de betrokkene wordt verstrekt. Zie over het helder informeren van betrokkenen ook de 'Richtsnoeren inzake transparantie' van de Groep gegevensbescherming artikel 29.[3]

Er zijn verschillende situaties waarin de betrokkene niet hoeft te worden geïnformeerd, namelijk als:

• de betrokkene al op de hoogte is van de informatie die anders verstrekt zou worden (artikel 13, vierde lid, AVG en artikel 14, vijfde lid, aanhef en onder a, AVG);
• het verstrekken van de informatie onmogelijk blijkt of onevenredig veel inspanning zou vergen, in het bijzonder bij verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden (deze uitzondering geldt alleen als de gegevens niet bij de betrokkene zijn verkregen);
• het voldoen aan de informatieverplichting de doelen van de verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen (deze uitzondering geldt alleen als de gegevens niet bij de betrokkene zijn verkregen);
• de vastlegging/verkrijging/verstrekking van de persoonsgegevens in nationaal of Europees recht is voorgeschreven en dat recht voorziet in passende maatregelen om de gerechtvaardigde belangen van de betrokkene te beschermen (deze uitzondering geldt alleen als de gegevens niet bij de betrokkene zijn verkregen);
• de persoonsgegevens vertrouwelijk moeten blijven uit hoofde van een beroepsgeheim (deze uitzondering geldt alleen als de gegevens niet bij de betrokkene zijn verkregen);
• zich een situatie voordoet als bedoeld in artikel 23 AVG jo. artikel 41 UAVG.

[3] Raadpleegbaar via https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp260rev01_nl.pdf.

Verder bevat de AVG een verbod op geautomatiseerde individuele besluitvorming – dat is: besluitvorming zonder menselijke tussenkomst – en enkele uitzonderingen op dat verbod (artikel 22 AVG jo. artikel 40 UAVG).

Tot slot moet een zogenoemde gegevensbeschermingseffectbeoordeling/privacy impact assessment worden uitgevoerd door een verwerkingsverantwoordelijke voorafgaand aan een verwerking die een hoog risico inhoudt voor de rechten en vrijheden van personen, zoals bij een structurele verstrekking van gevoelige persoonsgegevens (artikel 35 AVG e.v.) en moet rekening worden gehouden met de uitgangspunten van gegevensbescherming door ontwerp (data protection by design) en gegevensbescherming door standaardinstellingen (data protection by default) (artikel 25 AVG).[4]

De belangrijkste verplichtingen en aandachtspunten van de AVG bij het ontwikkelen van regietoepassingen volgen uit de bijgevoegde flowchart (**bijlage A**).

4.4 Verdieping AVG: toestemming als grondslag voor het verwerken van persoonsgegevens versus toestemming voor een regietoepassing

In de vorige paragraaf is reeds aangegeven dat voor iedere verwerking van persoonsgegevens een grondslag moet bestaan. Een van deze grondslagen is de toestemming van een betrokkene (artikel 6, eerste lid, aanhef en onder a, AVG) is. Om persoonsgegevens te kunnen verwerken op basis van toestemming is een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting van de betrokkene vereist (artikel 4, aanhef en onder 11, AVG). In aanvulling daarop is in de AVG vereist dat:

- De verwerkingsverantwoordelijke moet kunnen aantonen dat de betrokkene (geïnformeerd en actief) toestemming heeft gegeven (artikel 7, eerste lid, AVG);
- De betrokkene duidelijk moet worden geïnformeerd over het onderscheid tussen de toestemming en andere aangelegenheden (artikel 7, tweede lid, AVG) en tussen de verschillende verwerkingen waarvoor (specifieke) toestemming wordt gegeven;
- De betrokkene te allen tijde het recht heeft een gegeven toestemming in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerkingen op basis van de toestemming vóór de intrekking daarvan (artikel 7, derde lid, AVG); en
- Voor een vrije toestemming de betrokkene een echte en vrije keuze moet hebben (artikel 7, vierde lid, AVG). Toestemming is geen geldige grond voor het verwerken van persoonsgegevens als in een specifiek geval sprake is van een duidelijke wanverhouding tussen de verwerkingsverantwoordelijke en de

[4] Data protection by design betekent dat bij de ontwikkeling van producten en diensten (zoals nieuwe informatiesystemen) al zoveel mogelijk aandacht moet worden besteed aan privacy verhogende maatregelen en aan het uitgangspunt van dataminimalisatie. Data protection by default houdt in dat door middel van standaardinstellingen zo privacyvriendelijk mogelijk wordt gewerkt.

betrokkene, bijvoorbeeld in de relatie tussen een burger en een overheidsorgaan of bij een arbeidsverhouding.

Zie over toestemming als verwerkingsgrondslag in de zin van de AVG uitgebreider de 'Richtsnoeren inzake toestemming' van de Groep gegevensbescherming artikel 29.[5]

Toestemming als verwerkingsgrondslag in de zin van de AVG moet worden onderscheiden van het geven van toestemming ten behoeve van zeggenschap/regie over de eigen gegevens. Bij een regietoepassing zal soms toestemming van een betrokkene de verwerkingsgrondslag zijn voor het vloeien van gegevens in de zin van de AVG, maar in veel gevallen zal de AVG-grondslag een andere grondslag zijn, zoals de vervulling van een taak van algemeen belang die op die op de verwerkingsverantwoordelijke aanbieder rust (artikel 6, eerste lid, aanhef en onder e, AVG). Ook in dát geval zal het vanuit de principes voor regie op gegevens wenselijk zijn dat de betrokkene toestemming geeft voor het gebruik van de regietoepassing, maar dat is dan een andere toestemming dan toestemming in de zin van artikel 6, eerste lid, aanhef en onder a, AVG.

Wanneer in dit document wordt gesproken over *toestemming*, gaat het over de feitelijke toestemming voor regiehandelingen. Wanneer in dit document wordt gesproken over *toestemming als grondslag in de AVG*, wordt dit nadrukkelijk benoemd als toestemming in de zin van de AVG.

Het hierboven geschetste onderscheid doet er overigens niet af aan dat de eisen aan toestemming in de zin van de AVG bruikbaar zijn voor (waarborgen rondom) feitelijke toestemming voor regiehandelingen.

(Beleids)vraag voor de toekomst: is het wenselijk en haalbaar dat (bijvoorbeeld) door een centrale organisatie een toestemmingenoverzicht wordt bijgehouden, waarin burgers in een oogopslag kunnen zien voor welke regietoepassingen zij toestemming hebben gegeven?

4.5 Wet basisregistratie personen (Wet BRP)

Doel van de basisregistratie is overheidsorganen te voorzien van de in de registratie opgenomen gegevens, voor zover deze gegevens noodzakelijk zijn voor de vervulling van hun taak. Daarnaast kunnen derden worden voorzien van de in de registratie opgenomen gegevens in bij of krachtens de wet aangewezen gevallen (artikel 1.3 Wet BRP).

[5] Raadpleegbaar via: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp259_rev_0.1_nl.pdf.

Systematische verstrekkingen aan overheidsorganen (lees: bestuursorganen) op grond van de BRP geschiedt op verzoek van dat overheidsorgaan middels een autorisatiebesluit van de Minister van BZK. Overheidsorganen kunnen systematisch gegevens uit de BRP krijgen als zij deze gegevens nodig hebben voor de goede vervulling van hun taak (artikel 3.2 Wet BRP). Voorbeelden daarvan zijn de Belastingdienst, het UWV en de Sociale Verzekeringsbank.

Voor systematische verstrekkingen aan derden is relevant dat bij algemene maatregel van bestuur door derden verrichte werkzaamheden met een gewichtig maatschappelijk belang zijn aangewezen, ten behoeve waarvan gegevens uit de basisregistratie kunnen worden verstrekt (artikel 3.3 Wet BRP). De derden zijn aangeduid in bijlage 4 van het Besluit BRP (artikel 39 Besluit BRP). Het gaat onder meer om pensioenfondsen, zorgverzekeraars en ziekenhuizen.

Daarnaast kunnen er incidentele verstrekkingen plaatsvinden van gegevens uit de BRP. Deze verstrekkingen worden uitgevoerd door gemeenten. Gemeenten leggen in een verordening vast onder welke voorwaarden incidentele verstrekkingen plaatsvinden. Voorbeelden daarvan zijn de verstrekking van uittreksels uit de BRP aan de burger zelf, aan organen van de gemeente zoals de gemeentelijke belastingdienst (artikel 3.8 Wet BRP), aan andere bestuursorganen (artikel 3.5 Wet BRP), aan zgn. 'verplichte derden' zoals organisaties die gerechtelijke werkzaamheden uitvoeren (artikel 3.6 Wet BRP jo. artikel 41 Besluit BRP en bijlage 5) en (beperkt) aan andere derden (artikel 3.9 Wet BRP).

4.6 Wet algemene bepalingen burgerservicenummer (Wabb)

Overheidsorganen kunnen bij de uitvoering van hun taak gebruik maken van het Burgerservicenummer (BSN; artikel 10 Wabb) en moeten daar ook zoveel mogelijk gebruik van maken in de onderlinge communicatie (artikel 11 Wabb).

Anderen dan overheidsorganen kunnen alleen gebruik maken van het BSN voor zover dat bij of krachtens de wet is geregeld. Dat geldt bijvoorbeeld voor zorgverleners, huisartsen en zorgverzekeraars.

Denkbaar is dat aanbieders in het kader van een regietoepassing een document ter beschikking stellen aan de burger, waarbij het BSN wordt vermeld. Hoewel het de burger in dat geval vrijstaat het document te verstrekken aan de afnemer inclusief het BSN, zal niet iedere afnemer gelet op het voorgaande bevoegd zijn het BSN te verwerken.

4.7 eIDAS-verordening

De eIDAS-verordening richt zich op de betrouwbaarheid van elektronische identificatiemiddelen en op vertrouwensdiensten voor elektronische handtekeningen, elektronische zegels, elektronische tijdstempels, elektronische documenten, diensten

voor elektronisch aangetekende bezorging en certificatendiensten voor websiteauthenticatie (artikel 1 eIDAS-verordening).

Elektronische identificatiemiddelen

De eIDAS-verordening verplicht publieke organisaties en private organisaties met een publieke taak Europees erkende inlogmiddelen te accepteren binnen de digitale dienstverlening. Deze verplichting geldt onder meer voor organisaties die gebruik maken van DigiD (voor burgers) en eHerkenning (voor bedrijven).

Op basis van de verordening kan worden bepaald welk betrouwbaarheidsniveau is vereist.

> Zie Forum Standaardisatie, *Een handreiking voor overheidsorganisaties. Betrouwbaarheidsniveaus voor digitale dienstverlening*, april 2017, p. 23-25:

- Laag: als minimumeis geldt voor de identiteitsverificatie dat de gegevens kunnen worden gecontroleerd in de basisregistratie. Een middel met éénfactorauthenticatie volstaat.
- Substantieel: identiteitsverificatie vindt plaats doordat de gebruiker een geldig, officieel document bezit met dezelfde identiteitsgegevens die gecontroleerd kunnen worden in de basisregistratie. Tweefactorauthenticatie wordt vereist. Er moet sprake zijn van dynamische authenticatie: de (cryptografische) gegevens voor de authenticatie veranderen bij ieder gebruik.
- Hoog: de gebruiker moet ten minste eenmaal fysiek verschijnen.

Op basis van verschillende vragen kan worden bepaald welk niveau moet worden gekozen.

> Zie Forum Standaardisatie, *Een handreiking voor overheidsorganisaties. Betrouwbaarheidsniveaus voor digitale dienstverlening*, april 2017, p. 28-29:

1. Worden persoonsgegevens verwerkt en wat is de aard van de gegevens?
2. Wat zijn de rechtsgevolgen van het gebruik van de dienst?
3. Worden er basisregistratiegegevens gewijzigd?
4. Hoe groot is het economische belang bij de dienst?
5. Hoe groot is het publieke belang bij de dienst?

Criteria	Betrouwbaarheidsniveau (volgens eIDAS)
• Geen verwerking persoonsgegevens (klasse 0) • Geen BSN • Geen rechtsgevolg • Geen wijzigingen in basisregistratie • Economisch belang nihil • Publiek belang niet van toepassing	Geen eisen aan authenticatie
• Persoonsgegevens maximaal klasse 1 • BSN zelf verstrekt of impliciet in authenticatie • Mogelijk indirect rechtsgevolg • Alleen wijziging van niet risicovolle basisregistratiegegevens • Gering economisch belang • Publiek belang laag	Laag
• Persoonsgegevens maximaal klasse 2 • Verzwarende factor voor persoonsgegevens bovenop klasse 1 (aard verwerking) • BSN verwerkt in combinatie met aanvullende persoonsgegevens • Direct rechtsgevolg • Opgeven of wijzigen van basisregistratiegegevens die niet onder hoog vallen • Gemiddeld economisch belang • Gemiddeld publiek belang	Substantieel
• Persoonsgegevens klasse 3 • Verzwarende factor voor persoonsgegevens bovenop klasse 2 (aard verwerking) • BSN verwerkt in combinatie met aanvullende persoonsgegevens • Direct creëren, muteren of effectief beëindigen van (authentieke) basisregistratiegegevens • Groot economisch belang • Groot publiek belang	Hoog

Vetrouwensdiensten

De eIDAS-verordening is voorts van belang voor verleners van vertrouwensdiensten. Dat zijn diensten die het vertrouwen in online transacties bij bedrijven en consumenten vergroten, bijvoorbeeld certificaten voor elektronische handtekeningen, elektronische tijdstempels, elektronisch aangetekend bezorgen en certificaten voor de authenticatie van een website.

De verordening regelt de vereisten waaronder vertrouwensdiensten mogen worden aangeboden. Het Agentschap Telecom registreert vertrouwensdiensten en houdt toezicht.

4.8 Wet elektronisch bestuurlijk verkeer (Webv)

Met de Webv is afdeling 2.3 toegevoegd aan de Algemene wet bestuursrecht (Awb). Deze afdeling bevat algemene regels over het elektronisch verkeer tussen burgers en bestuursorganen. Uit artikel 2:14 Awb volgt dat een bestuursorgaan berichten alleen elektronisch aan geadresseerden kan zenden voor zover een geadresseerde kenbaar heeft gemaakt dat hij langs elektronische weg voldoende bereikbaar is. Daarnaast mag

een bericht nooit uitsluitend via de elektronische weg worden verzonden, tenzij bij wettelijk voorschrift is bepaald dat dit wel mag. Ook moeten berichten op een voldoende betrouwbare en vertrouwelijke manier worden verzonden.

Uit deze bepalingen volgt dat een bestuursorgaan niet zomaar berichten via elektronische weg aan een burger kan sturen. In de regel moet 1) de burger hebben aangegeven via die weg beschikbaar te zijn en 2) het bericht ook via andere (analoge) weg worden gezonden, tenzij bij wettelijk voorschrift anders is bepaald (zoals bijvoorbeeld bij de Berichtenbox van MijnOverheid).

Er is op dit moment een wetsvoorstel aanhangig om de bepalingen over elektronisch bestuurlijk verkeer te moderniseren.[6]

4.9 Algemene beginselen van behoorlijk bestuur

In het bestuursrecht zijn verschillende beginselen van toepassing die relevant kunnen zijn bij de inrichting en uitvoering van afsprakenstelsels en regietoepassingen, zoals het zorgvuldigheidsbeginsel (artikel 3:2 Awb), het motiveringsbeginsel (artikel 3:46 Awb), het evenredigheidsbeginsel (artikel 3:4, tweede lid, Awb), het gelijkheidsbeginsel en het verbod van détournement de pouvoir (artikel 3:3 Awb).

4.10 Geheimhoudingsplichten

In wet- en regelgeving zijn verschillende geheimhoudingsplichten vastgelegd. Zo geldt voor bestuursorganen dat een ieder die betrokken is bij de uitvoering van de taak van een bestuursorgaan en daarbij de beschikking krijgt over gegevens waarvan hij het vertrouwelijke karakter kent of redelijkerwijs moet vermoeden, in beginsel verplicht is tot geheimhouding van die gegevens (artikel 2:5 Awb). De geheimhoudingsplicht geldt niet als dat uit een wettelijk voorschrift of uit de taak van iemand volgt. Daarnaast bevat de Algemene wet inzake rijksbelastingen (AWR) een geheimhoudingsplicht voor fiscale gegevens (artikel 67 AWR) en de WGBO voor medische gegevens (artikel 7:457 BW). Ook contractueel kan geheimhouding overeen worden gekomen.

Per afsprakenstelsel en regietoepassing zal moeten worden nagegaan of een geheimhoudingsplicht aan de orde is en of er eventuele doorbrekingsgronden van toepassing (kunnen) zijn.

4.11 Vertegenwoordigen en machtigen in het BW en de Awb

Er zijn verschillende vormen van vertegenwoordiging:[7]

[6] Zie voor dit wetsvoorstel: *Kamerstukken II* 2018/19, 35 218, nr. 2.
[7] Hierna worden de algemene rechtsregels toegelicht omtrent vertegenwoordiging en machtiging gegeven. In sectorale wet- en regelgeving kunnen andere bepalingen omtrent vertegenwoordiging en machtiging zijn opgenomen. Zie bijvoorbeeld artikel 2.55 Wet basisregistratie personen.

1. Wettelijke vertegenwoordiging van handelingsonbekwamen, zoals minderjarigen door ouders en anderszins handelingsonbekwamen door een voogd, een curator een bewindvoerder of een executeur;
2. De vertegenwoordiging van rechtspersonen krachtens de wet en statuten; en
3. De vertegenwoordiging krachtens volmacht (artikel 3:60 t/m 3:79 BW).

Hieronder wordt eerst stilgestaan bij de regels voor de meest algemene vorm van vertegenwoordiging: de vertegenwoordiging krachtens volmacht. Vervolgens bespreken wij de regels voor vertegenwoordigen en machtigen in het bestuursrecht. Tot slot komen de wettelijk geregelde vormen van vertegenwoordiging voor handelingsonbekwamen en rechtspersonen kort aan de orde.

Vertegenwoordiging krachtens volmacht

Bij vertegenwoordiging krachtens volmacht verleent degene die vertegenwoordigd wil worden (de burger) een volmacht aan een gevolmachtigde (de vertegenwoordiger). De volmacht geeft de gevolmachtigde de bevoegdheid om namens de burger, uit zijn naam, rechtshandelingen te verrichten (artikel 3:60, eerste lid, BW).

Uitgangspunt is dat het verlenen van een volmacht vormvrij is, tenzij de wet anders bepaalt (artikel 3:61 BW). Dat betekent dat een volmacht ook mondeling kan worden verleend. Evenwel verdient het sterk de aanbeveling om een volmacht schriftelijk te verlenen. Op die manier wordt voorkomen dat er discussie ontstaat over de vraag óf er een volmacht is verleend.

In aanvulling daarop verdient het aanbeveling de inhoud van de volmacht – en daarmee de reikwijdte van de vertegenwoordigingsbevoegdheid – zo concreet mogelijk te omschrijven (artikel 3:62 BW). Op die manier kan zoveel mogelijk worden voorkomen dat er onduidelijkheid ontstaat over de reikwijdte van de volmacht.

Daarnaast moet het voor de burger ook duidelijk zijn waarvoor hij precies een volmacht verleent, en wat de implicaties daarvan zijn. Dat is allereerst vanuit juridisch perspectief relevant, omdat voor een rechtsgeldige volmachtsverlening een op rechtsgevolg gerichte wil van de burger is vereist, die zich door een verklaring heeft geopenbaard (artikel 3:33 en 3:35 BW). Daarnaast is het vanuit transparantieoogpunt van belang dat een burger weet wat de implicaties zijn van het inschakelen van een gevolmachtigde/vertegenwoordiger.

Wat gebeurt er als een vermeende gevolmachtigde handelt zonder volmacht of als de gevolmachtigde buiten zijn volmacht treedt? De burger kan in dat geval het onbevoegde handelen van de gevolmachtigde bekrachtigen (artikel 3:69 BW). Dat zal de burger echter niet altijd willen. Als de burger af wil van de rechtshandelingen die de gevolmachtigde onbevoegd heeft verricht, is de gevolmachtigde aansprakelijk voor de schade die een wederpartij leidt doordat de gevolmachtigde geen bevoegdheid had dan wel buiten zijn bevoegdheid is getreden (artikel 3:70 BW). De gevolmachtigde zal

dan ook eventuele schade moeten vergoeden, tenzij de wederpartij behoorde te begrijpen dat een toereikende volmacht ontbrak of de volledige inhoud van de volmacht aan de wederpartij was medegedeeld. Ook kan sprake zijn van wanprestatie in de relatie tussen de burger (de volmachtgever) en de gevolmachtigde.

Tot slot is de vraag hoe een volmacht kan eindigen. De burger kan een volmacht herroepen door een op beëindiging gerichte verklaring aan de gevolmachtigde (artikel 3:72 BW).[8] Het is ook daarbij weer van belang dat beëindiging van de volmacht geschiedt op duidelijke en ondubbelzinnige wijze. Volledigheidshalve wijzen wij op de in artikel 3:76 BW beschreven omstandigheden waarin de beëindiging van de volmacht niet aan de wederpartij kan worden tegengeworpen. Artikel 3:77 BW bevat regels voor rechtshandelingen die de gevolmachtigde verricht na overlijden van de burger .

Vertegenwoordiging in het bestuursrecht

De regels voor vertegenwoordiging en machtiging in het bestuursrecht zijn neergelegd in artikel 2:1 Awb. Op grond van de schakelbepaling van artikel 3:79 BW zijn de hierboven beschreven regels over volmachten ook van toepassing op vertegenwoordigers in het bestuursrecht. In de bestuursrechtelijke praktijk wordt daarbij doorgaans gesproken van "gemachtigden".

In aanvulling daarop is met name van belang dat een bestuursorgaan in het geval van een gemachtigde verplicht is het contact met de burger in beginsel via de gemachtigde te laten lopen. Het gaat dan niet alleen om de toezending van (formele) besluiten, maar ook om andere correspondentie.

Vertegenwoordiging van handelingsonbekwamen
Hierbij gaat het om de wettelijke vertegenwoordiging van handelingsonbekwamen, zoals minderjarigen door ouders en anderszins handelingsonbekwamen door een voogd, een curator een bewindvoerder of een executeur. De regels daaromtrent zijn primair neergelegd in boek 1 BW.

Vertegenwoordiging van rechtspersonen
Hierbij gaat het om de vertegenwoordiging van rechtspersonen krachtens de wet en statuten. De regels daaromtrent zijn primair neergelegd in boek 2 BW. De specifieke vertegenwoordigers om namens een rechtspersoon op te treden volgen uit de statuten.

4.12 Verantwoordelijkheden en aansprakelijkheden

Het wettelijk kader voor de verdeling van verantwoordelijkheden en aansprakelijkheden kent verschillende perspectieven. Het gaat dan in ieder geval om het gegevensbeschermingsperspectief en het aansprakelijkheidsperspectief.

[8] Een volmacht kan ook eindigen door opzegging van de gevolmachtigde en door dood, ondercuratelestelling, faillissement of schuldsanering aan de zijde van de burger of de gevolmachtigde (artikel 3:72 BW).

1) Verantwoordelijkheden vanuit gegevensbeschermingsperspectief

- Regeling gezamenlijke verwerkingsverantwoordelijken

Gezamenlijke verwerkingsverantwoordelijken moeten, zoals hierboven ook is opgemerkt, op grond van artikel 26 AVG een regeling treffen waarin zij op transparante wijze hun respectieve verantwoordelijkheden voor de nakoming van de verplichtingen uit hoofde van AVG moeten vaststellen, met name met betrekking tot de uitoefening van de rechten van de betrokkene[9] en hun respectieve verplichtingen om de in de artikelen 13 en 14 AVG bedoelde informatie te verstrekken. In de regeling kan een contactpunt voor betrokkenen worden aangewezen. Uit de regeling moet duidelijk blijken welke rol de gezamenlijke verwerkingsverantwoordelijken respectievelijk vervullen, en wat hun respectieve verhouding met de betrokkenen is. De wezenlijke inhoud van de regeling moet aan de betrokkene beschikbaar worden gesteld.

De gezamenlijke verwerkingsverantwoordelijken bij regietoepassingen zullen dan ook een regeling/document moeten opstellen waarin zij vastleggen hoe de nakoming van de AVG wordt gewaarborgd. Meer concreet zou onder andere gedacht kunnen worden aan afspraken over:

- de inhoud van de privacyverklaring, de wijze van het beschikbaar stellen van de privacyverklaring en de procedure voor het wijzigen en actualiseren van de privacyverklaring;
- tot wie de betrokkenen zich kunnen wenden indien zij hun rechten willen uitoefenen (bijv. hun inzage-, correctie- of verwijderingsrecht) en hoe uitvoering aan dergelijke verzoeken wordt gegeven;
- op welke wijze de verwerkingsverantwoordelijken zullen handelen in geval van een datalek;
- welke procedures moeten worden doorlopen om deel te kunnen nemen aan een regietoepassing, op welke wijze en door wie wordt beslist of een partij (niet langer) wordt toegelaten en wie die (beëindiging van de) toegang verwezenlijkt;
- de te stellen beveiligingseisen, op welke wijze beslissingen worden genomen over veranderingen in de beveiliging en over de controle op getroffen beveiligingsmaatregelen;
- welke bewaartermijnen zullen worden gehanteerd en hoe deze bewaartermijnen zullen worden nageleefd;
- wie het aanspreekpunt is in geval van een eventueel onderzoek van de AP;
- hoe de regeling bekend wordt gemaakt aan de betrokkenen.

[9] Zie voetnoot 2.

Het zou voor de hand liggen digitaal naar de regeling te verwijzen op de plaats waar bijvoorbeeld ook (voor het eerst) op de gebruikersvoorwaarden en de privacyverklaring wordt gewezen.

- Aanwijzen vertegenwoordiger bij regietoepassing met internationale component

De AVG is blijkens artikel 3 AVG van toepassing op, voor zover van belang:

- de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verwerkingsverantwoordelijke of een (sub)verwerker in de Europese Unie, ongeacht of de verwerking in de Europese Unie al dan niet plaatsvindt.

- de verwerking van persoonsgegevens van betrokkenen die zich in de Europese Unie bevinden, door een niet in de Europese Unie gevestigde verwerkingsverantwoordelijke of (sub)verwerker, wanneer de verwerking verband houdt met: a) het aanbieden van goederen of diensten aan deze betrokkenen in de Europese Unie, ongeacht of een betaling door de betrokkenen is vereist; of b) het monitoren van hun gedrag, voor zover dit gedrag in de Europese Unie plaatsvindt.

Als de laatstgenoemde situatie van toepassing is moet de verwerkingsverantwoordelijke of de (sub)verwerker – twee uitzonderingen daargelaten – schriftelijk een vertegenwoordiger in de Europese Unie aanwijzen. De vertegenwoordiger moet zijn gevestigd in een van de lidstaten waar zich de betrokkenen bevinden wier persoonsgegevens in verband met het hun aanbieden van goederen of diensten worden verwerkt, of wier gedrag wordt geobserveerd. De vertegenwoordiger moet door de verwerkingsverantwoordelijke of de (sub)verwerker worden gemachtigd om naast hem of in zijn plaats te worden benaderd, meer bepaald door de toezichthoudende autoriteiten en betrokkenen, over alle met de verwerking verband houdende aangelegenheden (artikel 27 AVG).

- Sluiten van verwerkersovereenkomsten

Op grond van artikel 28 AVG moet de verwerkingsverantwoordelijke met de verwerker een verwerkersovereenkomst sluiten, zoals hierboven ook reeds is aangegeven. Ook moet de eventuele (sub)verwerker een sub(sub)verwerkersovereenkomst sluiten. Vanzelfsprekend zal steeds in de gaten moeten worden gehouden of nieuwe ontwikkelingen ertoe leiden dat er nieuwe of andere verwerkers bij komen.

De verwerkersovereenkomst dient in ieder geval de volgende informatie te bevatten:

- een garantie van de verwerker met betrekking tot het toepassen van passende technische en organisatorische maatregelen opdat de verwerking

aan de vereisten van de AVG voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd (artikel 28, eerste lid, AVG);

- een beschrijving van het onderwerp, de duur, de aard en het doel van de verwerkingen die plaatsvinden (artikel 28, derde lid, AVG);
- een beschrijving van het soort persoonsgegevens dat wordt verwerkt (artikel 28, derde lid, aanhef AVG);
- een beschrijving van de categorieën van betrokkenen waarop de persoonsgegevens die verwerkt worden zien (artikel 28, derde lid, AVG);
- de verplichting dat de verwerker de persoonsgegevens uitsluitend verwerkt op basis van schriftelijke instructies van de verwerkingsverantwoordelijke, onder meer met betrekking tot doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, tenzij een unierechtelijke of lidstaatrechtelijke bepaling tot verwerking verplicht, in welk geval de verwerker de verwerkingsverantwoordelijke voorafgaand aan de verwerking van dat wettelijke voorschrift in kennis stelt (tenzij die wetgeving die kennisgeving om gewichtige redenen van algemeen belang verbiedt) (artikel 28, derde lid, aanhef en onder a AVG);
- de verplichting dat de verwerker waarborgt dat de tot het verwerken van de persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting tot vertrouwelijkheid zijn gebonden (artikel 28, derde lid, aanhef en onder b AVG);
- de verplichting dat de verwerker passende technische en organisatorische beveiligingsmaatregelen treft (artikel 28, derde lid, aanhef en onder c jo. artikel 32 AVG);
- de verplichting dat de verwerker zonder voorafgaande specifieke of algemene schriftelijke toestemming van de verwerkingsverantwoordelijke geen subverwerker mag inschakelen. En de verplichting dat, in het geval van algemene schriftelijke toestemming, de verwerker de verwerkingsverantwoordelijke inlicht over beoogde veranderingen inzake de toevoeging of vervanging van subverwerkers, waarbij de verwerkingsverantwoordelijke de mogelijkheid heeft om bezwaar te maken (artikel 28, derde lid, aanhef en onder d jo. artikel 28, tweede lid, AVG);
- de verplichting de verwerker met subverwerkers een rechtsgeldige verwerkersovereenkomst sluit met daarin dezelfde verplichtingen als waaraan de verwerker jegens de verwerkingsverantwoordelijke is gebonden (artikel 28, derde lid, aanhef en onder d jo. artikel 28, vierde lid, AVG);
- de verplichting dat de verwerker, rekening houdend met de aard van de verwerking, de verwerkingsverantwoordelijke door middel van passende technische en organisatorische maatregelen, voor zover mogelijk, bijstand verleent bij het vervullen van diens plicht om verzoeken tot uitoefening van de in hoofdstuk III van de AVG vastgestelde rechten van de betrokkene te beantwoorden (artikel 28, derde lid, aanhef en onder e, AVG);
- de verplichting dat de verwerker de verwerkingsverantwoordelijke bijstand verleent bij het voldoen aan zijn verplichting om uiterlijk binnen 72 uur na

ontdekking een datalek te melden bij de Autoriteit Persoonsgegevens op de wijze als beschreven in artikel 33 AVG en om een datalek te melden aan de betrokkene overeenkomstig op de wijze als beschreven in artikel 34 AVG (artikel 28, derde lid, aanhef en onder f jo. artikel 33 en 34 AVG);

- de verplichting dat de verwerker de verwerkingsverantwoordelijke bijstand verleent bij het uitvoeren van de gegevensbeschermingseffectbeoordeling als bedoeld in artikel 35 AVG (artikel 28, derde lid, aanhef en onder f jo. artikel 35 AVG);
- de verplichting dat de verwerker de verwerkingsverantwoordelijke bijstand verleent bij het uitvoeren van een voorafgaande raadpleging als bedoeld in artikel 36 AVG (artikel 28, derde lid, aanhef en onder f jo. artikel 36 AVG);
- de verplichting dat de verwerker, afhankelijk van de keuze van de verwerkingsverantwoordelijke, alle persoonsgegevens wist of terugbezorgt en bestaande kopieën verwijdert, tenzij opslag van de persoonsgegevens Unierechtelijk of lidstaatrechtelijk is verplicht (artikel 28, derde lid, aanhef en onder g AVG);
- de verplichting dat de verwerker om de verwerkingsverantwoordelijke alle informatie ter beschikking te stellen die nodig is om de nakoming van de in artikel 28 AVG neergelegde verplichtingen aan te tonen en audits, waaronder inspecties, door de verwerkingsverantwoordelijke of een door de verwerkingsverantwoordelijke gemachtigde controleur mogelijk te maken en eraan bij te dragen (artikel 28, derde lid, aanhef en onder h AVG); en
- de verplichting dat de verwerker en eenieder die onder diens gezag handelt de persoonsgegevens uitsluitend in opdracht van de verwerkingsverantwoordelijke verwerkt (artikel 29 AVG).

Verder is van belang dat artikel 82 AVG een bepaling bevat voor een recht op schadevergoeding als gevolg van overtreding van de AVG.

2) Verantwoordelijkheden vanuit aansprakelijkheidsperspectief

- Contractuele aansprakelijkheid

Denkbaar is dat binnen sectorale afsprakenstelsels of bij regietoepassingen overeenkomsten worden gesloten tussen de verschillende actoren, waarin bijvoorbeeld (gebruiks)voorwaarden worden opgenomen. Indien een van de partijen in strijd met die overeenkomst handelt, kan dat leiden tot wanprestatie en mogelijk tot een verplichting schade te vergoeden (artikel 6:74 BW e.v.).

- Buiten-contractuele aansprakelijkheid

Als er iets fout gaat buiten een overeenkomst om, kan dat leiden tot aansprakelijkheid uit onrechtmatige daad. Daarvoor gelden de algemene normen van artikel 6:162 BW e.v.

Op basis van specifieke(re) casuïstiek kan een juridisch oordeel worden gegeven over de vraag wie wanneer aansprakelijk is voor fouten in de uitvoering bij een regietoepassing. Daarvoor is onder meer bepalend:

- Of en zo ja, welke afspraken er tussen partijen gelden (door welke wet- en regelgeving wordt de verhouding tussen partijen beheerst? Zijn er contractuele afspraken gemaakt of niet?);
- Hoe gegevens feitelijk vloeien tussen partijen (berusten de gegevens bij de betrokkene? Of vloeien deze rechtstreeks van de aanbieder naar de afnemer?);
- Waar de onrechtmatige handeling of het nalaten plaatsvindt (is er sprake van een datalek en zo ja, bij wie? Zijn gegevens misbruikt voor ongeoorloofde doeleinden?)

4.13 Mededinging en de Wet Markt en Overheid (Wet M&O)

Uitgangspunt van de Wet M&O is dat de overheid in de hoedanigheid van ondernemer diensten en werkzaamheden op de markt kan aanbieden. Als de overheid daarmee economische activiteiten verricht en zich gedraagt als een onderneming, dan is dat slechts toegestaan indien en voor zover de overheid daarbij vier gedragsregels in acht neemt: integrale kostendoorberekening; verbod bevoordeling overheidsbedrijven; gelijk gebruik van gegevens; en functiescheiding tussen bestuurlijke en economische activiteiten.

Meer in het algemeen, dus los van de Wet Markt en Overheid, geldt dat de overheid een gelijk speelveld moet waarborgen als zij gegevens gaat delen met de markt. Zo kan de overheid/een overheidsorgaan binnen een regietoepassing optreden als “facilitator”. De overheid is in dat geval degene die een regietoepassing mogelijk maakt, bijvoorbeeld door gegevens te laten stromen via een overheidsplatform. Uitgangspunt moet daarbij zijn dat ondernemingen gelijke kansen hebben om daaraan deel te nemen, en dus bijvoorbeeld niet een bedrijf wel en een ander bedrijf geen gebruik mag maken van het platform, zonder dat er gerechtvaardigde redenen zijn voor dat onderscheid. Dergelijke gelijke kansen kan een overheidsorgaan bieden door bijvoorbeeld:

- Transparant te zijn over het voornemen om deel te nemen aan de regietoepassing, bijvoorbeeld door het voornemen om deel te gaan nemen te publiceren;
- Een open samenwerking te creëren waaraan iedereen onder bepaalde voorwaarden mag deelnemen;
- Resultaten van de samenwerking zoveel mogelijk publiekelijk te delen; en
- Anderen de mogelijkheid te bieden om tussentijds toe te treden tot de samenwerking.

Ook als de overheid optreedt in de rol van gegevensverstrekker (aanbieder) is het uitgangpunt gelijke kansen voor verschillende marktpartijen. Het kan dus niet zo zijn dat de ene partij wel gebruik kan maken van gegevens van de overheid en de andere partij niet, zonder dat er gerechtvaardigde redenen zijn voor dat onderscheid.

Verder kan samenwerking *tussen* aanbieders nadere aandacht behoeven en moet rekening worden gehouden met de regels voor (immateriële) staatssteun.

4.14 Archiefwet

De Archiefwet (en het daarop gebaseerde Archiefbesluit en de Archiefregeling) bevat regels voor overheidsorganen met betrekking tot het bewaren en vernietigen van overheidsinformatie. Uit de archiefwet- en regelgeving volgt dat ieder overheidsorgaan een selectielijst moet vaststellen waarin tenminste wordt aangegeven welke archiefbescheiden voor vernietiging in aanmerking komen en welke termijnen daarvoor gelden.

Deze verplichting geldt voor onder het overheidsorgaan berustende archiefbescheiden, en niet voor bescheiden die door verstrekking onder een andere (niet-overheids)partij zijn komen te berusten (zoals bij een afnemer).

4.15 Tijdelijk besluit digitale toegankelijkheid overheid

Overheden bieden steeds meer dienstverlening aan op digitale wijze. Om de toegankelijkheid van deze digitale dienstverlening voor mensen met een functiebeperking (bijvoorbeeld een visuele, auditieve en/ of cognitieve beperking) te waarborgen, heeft de regering vorig jaar het Tijdelijk besluit digitale toegankelijkheid overheid genomen. Op grond van het Tijdelijk besluit moeten vrijwel alle overheidswebsites en mobiele applicaties van overheden aan bepaalde toegankelijkheidsnormen voldoen. Een groot deel van de overheidswebsite moet vanaf 23 september 2019 aan de toegankelijkheidsnormen voldoen.

4.16 Diverse wet- en regelgeving voor bronnen van aanbieders

In aanvulling op het voorgaande zullen bepaalde aanbieders van gegevens (ook wel genoemd: bronhouders) aan specifieke wet- en regelgeving zijn gebonden met betrekking tot het verstrekken van gegevens. Gedacht kan worden aan het kadaster (Kadasterwet), de Kamer van Koophandel (Wet op de Kamer van Koophandel) en de Belastingdienst (artikel 67 AWR).

Voorbeeld Belastingdienst

Aangezien de Belastingdienst over een groot aantal privacygevoelige gegevens beschikt, is de geheimhoudingsplicht strikt. In artikel 67 AWR is geregeld dat iedereen die zich met enige werkzaamheid bij de uitvoering van de

belastingwet bezighoudt, in principe alles geheim moet houden. Alles wat hij in dat kader ziet, opmerkt of te horen krijgt, mag hij in beginsel niet aan derden doorgeven. Informatie bekendmaken mag alleen als dat noodzakelijk is voor de uitvoering van de belastingwet en de invordering van belastingschulden. Een belangrijke bepaling, want het kan niet de bedoeling zijn dat alle informatie die belastingplichtigen moeten verstrekken vervolgens vrijelijk aan anderen ter beschikking wordt gesteld. De achtergrond van de bepaling is ook dat niemand door de vrees dat de gegevens voor iets anders dan het vaststellen van een juiste heffing worden gebruikt, moet worden weerhouden van het verstrekken van informatie aan de Belastingdienst.

Op deze geheimhoudingsplicht bestaan vier uitzonderingen:
1. de wettelijke verplichting tot bekendmaking;
2. de noodzakelijke bekendmaking ten behoeve van een goede vervulling van publiekrechtelijke taken. Dat moet bij ministeriële regeling zijn bepaald;
3. bekendmaking aan degene op wie zij betrekking hebben, maar alleen voor zover de gegevens door of namens hem zijn verstrekt;
4. in geval van ontheffing door de Minister.

(Beleids)vraag voor de toekomst: bronhouders hebben behoefte aan duiding over de vraag onder welke omstandigheden zij welke gegevens mogen verstrekken en aan wie. Veel van die vragen moeten worden beantwoord op basis van sectorale wet- en regelgeving. Het is raadzaam voor iedere relevante bronhouder een ‘landschapskaart’ te maken waarop de verschillende mogelijke gegevensreizen per bronhouder worden weergegeven. Alleen op die wijze kan inzicht worden verkregen in de toelaatbaarheid van iedere reis van een gegeven uit een bron.

5 (Juridische inspiratie voor) afspraken/spelregels

5.1 Inleiding

In aanvulling op of bij gebreke aan wet- en regelgeving moeten afspraken worden gemaakt om op verantwoorde wijze vorm te geven aan regie op gegevens. Als gezegd, is de mate waarin die afspraken/spelregels van toepassing zijn afhankelijk van de mate waarin het betreffende afsprakenstelsel of de betreffende regietoepassing al wettelijk is gereguleerd.

Hieronder wordt eerst ingegaan op enkele algemene overwegingen voor te maken afspraken/op te stellen spelregels voor regie op gegevens (paragraaf 5.2).

Daarna wordt per principe ingegaan op de verschillende vraagstukken die spelen bij dat principe.[10] Voor ieder vraagstuk worden de afspraken/spelregels geformuleerd die daarvoor kunnen gaan gelden, met bijbehorende juridische onderbouwing of juridische inspiratie. Achtereenvolgend komen de volgende principes met bijbehorende vraagstukken aan bod:

- Transparantie (paragraaf 5.3);
- Vertrouwen (paragraaf 5.4);
- Interoperabiliteit (paragraaf 5.5);
- Gegevenskwaliteit (paragraaf 5.6);
- Het voorkomen van druk op het (digitaal) delen van gegevens (paragraaf 5.7); en
- Betalen voor gegevens (paragraaf 5.8).

5.2 Denkkader algemeen: regie op gegevens en de AVG

Vooropgesteld wordt dat alle afsprakenstelsels en regietoepassingen moeten voldoen aan de daarvoor geldende generieke wet- en regelgeving (zie ook hoofdstuk 4). Een van die wetten is de AVG, die (kort gezegd) van toepassing is als bij regie op gegevens persoonsgegevens worden verwerkt. Maar ook om tot (aanvullende) afspraken/spelregels te komen die niet zozeer of niet alleen zien op de verwerking van persoonsgegevens, kan de geest van de AVG worden gevolgd.

Zo kunnen ook bij het vloeien van andere gegevens dan persoonsgegevens verwerkingsverantwoordelijken en verwerkers worden aangewezen, die met elkaar afspraken moeten maken over de respectieve verantwoordelijkheden (de rollen).

Ook voor de regiehandelingen inzage, correctie en delen kan de geest van de AVG worden gevolgd, in die zin dat personen zoveel mogelijk in de positie worden gebracht

[10] Zoals aangegeven in de inleiding (hoofdstuk 1) is dit juridisch kader beperkt tot de (onderbouwing van) afspraken/spelregels die een relatie hebben met bestaande wet- en regelgeving.

dat voor hen inzichtelijk is welke gegevens, door wie, met welk doel, op welke wijze worden verwerkt.

Verder moeten in ieder geval ook de waarborgen van de AVG inzake de beginselen van verwerking van persoonsgegevens – te weten: de beginselen van doelbinding, dataminimalisatie, juistheid, opslagbeperking en integriteit en vertrouwelijkheid – tot uitgangspunt worden genomen bij de verwerking van gegevens.

5.3 Transparantie

Vraagstuk: de begrijpelijkheid van regietoepassingen, ook voor kwetsbare groepen

Afspraak/spelregel voor de begrijpelijkheid van regietoepassingen, ook voor kwetsbare groepen:

Alle informatie over een regietoepassing moet in beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en eenvoudige taal worden aangeleverd. Daarbij wordt zoveel mogelijk gebruik gemaakt van toegankelijkheidsstandaarden en visualisaties.

Onderbouwing

1. Tijdelijk besluit digitale toegankelijkheid overheid

Overheden bieden steeds meer dienstverlening aan op digitale wijze. Om de toegankelijkheid van deze digitale dienstverlening voor mensen met een functiebeperking (bijvoorbeeld een visuele, auditieve en/ of cognitieve beperking) te waarborgen, heeft de regering vorig jaar het Tijdelijk besluit digitale toegankelijkheid overheid genomen. Op grond van het Tijdelijk besluit moeten vrijwel alle overheidswebsites en mobiele applicaties van overheden aan bepaalde toegankelijkheidsnormen voldoen. Een groot deel van de overheidswebsite moet vanaf 23 september 2019 aan de toegankelijkheidsnormen voldoen.

Let wel: dit besluit heeft alleen betrekking op overheidsinstanties.

2. AVG

Ook uit de AVG volgt dat een betrokkene communicatie in verband met de verwerking van persoonsgegevens in een “beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm” moet ontvangen, evenals in “eenvoudige taal” (artikel 12, eerste lid, AVG).

5.4 Vertrouwen

Vraagstuk 1: security en privacy

Afspraak/spelregel voor security en privacy:

- Deelnemende partijen treffen beveiligingsmaatregelen die passen bij de gegevens die worden verwerkt. Daarbij wordt in ieder geval rekening gehouden met:
  - De aard van de gegevens: betreffen dat gevoelige gegevens, zoals inkomensgegevens of gezondheidsgegevens?
  - De omvang van de verwerking: gaat het om grote hoeveelheden gegevens?

- Deelnemende partijen beschrijven de maatregelen voor gegevensbescherming en maken die kenbaar aan zowel de burger als de andere deelnemende partijen.

Onderbouwing

1. AVG

De aanbieder en afnemer moeten de nodige beveiligingsmaatregelen treffen om (de verwerking van) persoonsgegevens te beschermen (artikel 5, eerste lid, aanhef en onder f, AVG en artikel 32 AVG). De aan de verwerking inherente risico's moeten worden beoordeeld en maatregelen, zoals versleuteling, moeten worden getroffen om die risico's te beperken. Die maatregelen dienen een passend niveau van beveiliging te waarborgen, rekening houdend met de stand van de techniek en de uitvoeringskosten afgezet tegen de risico's en de aard van de te beschermen persoonsgegevens (considerans 83 AVG). Dit resulteert eveneens in de plicht tot het blijven monitoren van het beveiligingsniveau.

Ook moeten de aanbieders en afnemers de nodige beveiligingsafspraken maken met eventuele verwerkers. Dat moet in een zogenoemde verwerkersovereenkomst (artikel 28, derde lid, AVG). Daarin moet onder meer het volgende worden bepaald:

- De verwerker moet waarborgen dat alle personen die gemachtigd zijn persoonsgegevens te verwerken vertrouwelijkheid in acht nemen;
- De verwerker alle te treffen beveiligingsmaatregelen neemt (artikel 32 AVG);
- De verwerker de verwerkingsverantwoordelijke bijstand verleent bij de melding van eventuele datalekken (artikel 33 en 34 AVG) en bij uit te voeren DPIA's (artikel 35 en 36 AVG)

Vraagstuk 2: Identificatie, Authenticatie en Autorisatie (IAA)

Afspraak/spelregel voor identificatie, Authenticatie en Autorisatie:

Partijen zijn gehouden aan de normen uit de eIDAS-verordening. Identificatie en authenticatie zal daarom plaatsvinden aan de hand van een identificatiemiddel op het juiste betrouwbaarheidsniveau.

Zie voor de onderbouwing paragraaf 4.7 van dit juridisch kader over de eIDAS-verordening.

Vraagstuk 3: het gebruik van BSN[11]

Afspraak/spelregel voor het gebruik van BSN:

- Vanuit het oogpunt van dataminimalisatie verdient het de voorkeur dat alleen *gegevens* vloeien bij regietoepassingen, en niet *documenten* met gegevens. Documenten zullen veelal meer gegevens bevatten dan de afnemer nodig heeft, zoals het BSN;
- Aanbieders kunnen nooit rechtstreeks het BSN/documenten met het BSN aan afnemers verstrekken die niet bevoegd zijn het BSN te verwerken;
- Er zullen vooralsnog regietoepassingen zijn waarbij documenten vloeien, zoals pdf-bestanden, in plaats van sec gegevens. Dergelijke documenten kunnen het BSN van een burger bevatten. Afnemers die niet bevoegd zijn het BSN te verwerken, moeten in de aangewezen gevallen de burger verzoeken om – al dan niet met behulp van technische tools (vgl. de paspoort-tool) – documenten zonder BSN aan te leveren. Het gaat daarbij om gevallen waarin het voor de hand ligt dat de informatie die de afnemer verlangt het BSN van de burger bevat;
- Intermediairs die in opdracht van de burger gegevens verwerken, verwerken het BSN alleen voor zover zij daartoe gerechtigd zijn.

[11] Zie over de verwerking van nationale identificatienummers, waaronder het BSN ook p. 15 van dit juridisch kader.

Onderbouwing

1. Wet algemene bepalingen burgerservicenummer (Wabb)

Overheidsorganen kunnen bij de uitvoering van hun taak gebruik maken van het Burgerservicenummer (BSN; artikel 10 Wabb) en moeten daar ook zoveel mogelijk gebruik van maken in de onderlinge communicatie (artikel 11 Wabb).

Anderen dan overheidsorganen kunnen alleen gebruik maken van het BSN voor zover dat bij of krachtens de wet is geregeld. Dat geldt bijvoorbeeld voor zorgverleners, huisartsen en zorgverzekeraars.

Denkbaar is dat aanbieders in het kader van een regietoepassing een document ter beschikking stellen aan de burger , waarbij het BSN wordt vermeld. Hoewel het de burger in dat geval vrijstaat het document te verstrekken aan de afnemer inclusief het BSN, zal niet iedere afnemer gelet op het voorgaande bevoegd zijn het BSN te verwerken.

Vraagstuk 4: voorzieningen voor machtigen

Afspraak/spelregel voor voorzieningen voor machtigingen/volmachten:

- een volmacht moet schriftelijk worden verleend;
- in de volmacht wordt duidelijk en concreet omschreven wat de reikwijdte van de volmacht is; en
- de burger wordt in begrijpelijke taal geïnformeerd over de inhoud van de volmacht en de implicaties daarvan, evenals over de mogelijkheid om de volmacht te herroepen.

Onderbouwing

1. Vertegenwoordiging krachtens volmacht

Bij vertegenwoordiging krachtens volmacht verleent degene die vertegenwoordigd wil worden (de burger) een volmacht aan een gevolmachtigde (de vertegenwoordiger). De volmacht geeft de gevolmachtigde de bevoegdheid om namens de burger , uit zijn naam, rechtshandelingen te verrichten (artikel 3:60, eerste lid, BW).

Uitgangspunt is dat het verlenen van een volmacht vormvrij is, tenzij de wet anders bepaalt. Dat betekent dat een volmacht ook mondeling kan worden verleend. Evenwel verdient het sterk de aanbeveling om een volmacht schriftelijk te verlenen. Op die

manier wordt voorkomen dat er discussie ontstaat over de vraag óf er een volmacht is verleend.

In aanvulling daarop verdient het aanbeveling de inhoud van de volmacht – en daarmee de reikwijdte van de vertegenwoordigingsbevoegdheid – zo concreet mogelijk te omschrijven. Op die manier kan zoveel mogelijk worden voorkomen dat er onduidelijkheid ontstaat over de reikwijdte van de volmacht.

Daarnaast moet het voor de burger ook duidelijk zijn waarvoor hij precies een volmacht verleent, en wat de implicaties daarvan zijn. Dat is allereerst vanuit juridisch oogpunt relevant, omdat voor een rechtsgeldige volmachtsverlening een op rechtsgevolg gerichte wil van de burger vereist, die zich door een verklaring heeft geopenbaard (artikel 3:33 en 3:35 BW). Daarnaast is het gewoonweg vanuit transparantieoogpunt van belang dat een burger weet wat de implicaties zijn van het inschakelen van een gevolmachtigde/vertegenwoordiger. De eis kan daarom worden genomen dat een volmacht niet alleen schriftelijk moet worden verleend met een concrete omschrijving van de reikwijdte van de volmacht, maar ook dat de inhoud van de volmacht en de implicaties daarvan in begrijpelijke taal wordt aangereikt aan de burger.

Wat gebeurt er als een vertegenwoordiger handelt zonder volmacht of als de vertegenwoordiger buiten zijn volmacht treedt? De burger kan onbevoegd handelen achteraf bekrachtigen (artikel 3:69 BW). Dat zal de burger echter niet altijd willen. Als de burger af wil van de rechtshandelingen die de gevolmachtigde onbevoegd heeft verricht, is de gevolmachtigde aansprakelijk voor de schade die een wederpartij leidt doordat de gevolmachtigde geen bevoegdheid had dan wel buiten zijn bevoegdheid is getreden (artikel 3:70 BW). De gevolmachtigde zal dan ook eventuele schade moeten vergoeden, tenzij de wederpartij behoorde te begrijpen dat een toereikende volmacht ontbrak of de volledige inhoud van de volmacht aan de wederpartij was medegedeeld. Ook kan sprake zijn van wanprestatie in de relatie tussen de burger (de volmachtgever) en de gevolmachtigde.

Tot slot is de vraag hoe een volmacht kan eindigen. De burger kan een volmacht herroepen door een op beëindiging gerichte verklaring aan de gevolmachtigde. Het is ook daarbij weer van belang dat beëindiging van de volmacht geschiedt op duidelijke en ondubbelzinnige wijze (artikel 3:72 BW).[12] Volledigheidshalve wijzen wij op de in artikel 3:76 BW beschreven omstandigheden waarin de beëindiging van de volmacht niet aan de wederpartij kan worden tegengeworpen. Artikel 3:77 BW bevat regels voor rechtshandelingen die de gevolmachtigde verricht na overlijden van de burger.

[12] Een volmacht kan ook eindigen door opzegging van de gevolmachtigde en door dood, ondercuratelestelling, faillissement of schuldsanering aan de zijde van de burger of de gevolmachtigde (artikel 3:72 BW).

2. Vertegenwoordiging in het bestuursrecht

De regels voor vertegenwoordiging en machtiging in het bestuursrecht zijn neergelegd in artikel 2:1 Awb. Op grond van de schakelbepaling van artikel 3:79 BW zijn de hierboven beschreven regels over volmachten ook van toepassing op vertegenwoordigers in het bestuursrecht. In de bestuursrechtelijke praktijk wordt daarbij doorgaans gesproken van “gemachtigden”.

In aanvulling daarop is met name van belang dat een bestuursorgaan in het geval van een gemachtigde verplicht is het contact met de burger in beginsel via de gemachtigde te laten lopen. Het gaat dan niet alleen om de toezending van (formele) besluiten, maar ook om andere correspondentie.

5.5 Interoperabiliteit

Vraagstuk: technologie- en platform onafhankelijke vragen

Afspraak/spelregel voor technologie- en platform onafhankelijk vragen:

Verschillende technologieën roepen ieder eigen juridische en organisatorische vragen op door de diverse technologische standaarden die aan de orde zijn. Bij de implementatie van een regietoepassing moet daar aandacht voor zijn en moet een aanvullende toets plaatsvinden.

Onderbouwing

Het voeren van regie op gegevens zal niet op papier gaan, maar digitaal. Dat roept vragen op over de wijze waarop die digitale tool technisch wordt geïmplementeerd. Zo draait MedMij bijvoorbeeld op een bepaald platform, kan MijnOverheid wellicht als platform voor regie worden gebruikt en zijn er talloze andere opties, zoals bijvoorbeeld ook blockchain-technologie.

5.6 Gegevenskwaliteit- en hoeveelheid

Vraagstuk 1: gebruik van authentieke bronnen

Afspraak/spelregel voor het gebruik van authentieke bonnen:

Binnen een afsprakenstelsel of regietoepassing wordt gewerkt met ofwel authentieke gegevens (rechtstreeks uit de bron) ofwel geverifieerde kopieën. Het betreffen steeds digitale, gewaarmerkte gegevens.

Het volgende wordt daarbij in acht genomen:

- Voorkomen wordt dat de gegevens onjuist of verouderd zijn, bijvoorbeeld door de gegevens regelmatig te verversen; en
- Verstrekking van gegevens gaat altijd gepaard met een bronvermelding en timestamp.

Desgewenst kan een aanbieder ook afspraken maken met een afnemer over:

- de verantwoordelijkheid van de afnemer voor het gebruik van de gegevens;
- de verplichting om te voldoen aan relevante maatregelen, bijvoorbeeld ten aanzien van beveiliging, log-in en de terugmeldplicht in het geval van gerede twijfel over de juistheid van een gegeven; en
- een controlemechanisme waardoor afwijkingen tussen de bron en de kopie kunnen worden opgemerkt en opgelost.

Onderbouwing

1. AVG

Voor de verwerking van persoonsgegevens is in de AVG bepaald dat een verwerkingsverantwoordelijke maatregelen moet treffen die waarborgen dat de persoonsgegevens die zij verwerken juist en actueel zijn. Dit volgt uit artikel 5, eerste lid, aanhef en onder d, AVG, waarin kort gezegd is bepaald dat persoonsgegevens juist moeten zijn en zo nodig moeten worden geactualiseerd.

Een verwerkingsverantwoordelijke moet op grond van artikel 5, eerste lid, aanhef en onder d, AVG alle redelijke maatregelen nemen om persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren.

2. Authentieke gegevens uit basisregistraties

Overheidsinstellingen zijn verplicht gebruik te maken van authentieke gegevens uit basisregistraties. In de wet van een basisregistratie, waaronder bijvoorbeeld in de wet voor de BRP, voor het Handelsregister en voor de Basisregistratie Inkomen, ligt vast welke gegevens authentiek zijn. Enkele basisregistraties bieden de mogelijkheid om gegevenskopieën te gebruiken. De ratio achter dit soort basisregistraties, die worden beheerd door overheidsorganen, is – kort gezegd – een zekere mate van betrouwbaarheid en zekerheid over de daarin opgenomen gegevens.

Commerciële derden zouden zich echter kunnen aanbieden om – goedkoper en/of sneller – gegevens te verstrekken uit secundaire bronnen. Het risico van dit soort secundaire bronnen is dat afwijkingen kunnen ontstaan tussen de authentieke bron(gegevens) en de gegevens in de secundaire bronnen, zonder dat die discrepantie eenvoudig kan worden hersteld. De secundaire bron is immers niet of nauwelijks gereguleerd en er kunnen meerdere secundaire bronnen met dezelfde foutieve gegevens bestaan (zie daarover ook het rapport 'Kopiebestanden. Status en positionering van gegevenskopieën' van 2013 vanuit het Programma i-NUP). Die risico's worden nog groter als er besluiten worden genomen op basis van die foutieve gegevens uit de secundaire bron (bijvoorbeeld wel/geen woning) of er verkeerde interconnecties, verbindingen of koppelingen worden gemaakt.

Ook buiten het overheidsveld, en buiten de wettelijk voorgeschreven basisregistraties, verdient het daarom aanbeveling dat zoveel mogelijk met authentieke gegevens wordt gewerkt.

Overigens is het niet altijd mogelijk om authentieke gegevens te gebruiken en, dus, het werken met kopieën van (bron)gegevens volledig uit te sluiten. Kopieën maken het bijvoorbeeld mogelijk om gegevens uit basisregistraties te combineren met andere basisregistraties of met andere registraties. In sommige gevallen is van groot belang dat de afnemer en/of de burger niet afhankelijk is van de systemen van de basisregistratie, bijvoorbeeld als de afnemer een kopie wil gebruiken in eigen processen. Zonder kopie zullen complexe processen bij de afnemer alleen goed uit te voeren zijn als de bronhouders deze processen zou ondersteunen.

3. eIDAS-verordening

Vertrouwensdiensten in de zin van de eIDAS-verordening kunnen een rol spelen bij het vertrouwen in de gegevens die worden verstrekt, bijvoorbeeld door validatie van gekwalificeerde elektronische handtekeningen.

Vraagstuk 2: dataminimalisatie

Afspraak/spelregel voor dataminimalisatie:

Zowel de aanbieder als de afnemer hebben een verantwoordelijkheid om niet meer gegevens te verwerken dan nodig voor de dienst die wordt geleverd.

De afnemer wordt verplicht om een concrete (gegevens uit)vraag te stellen aan burgers.

Onderbouwing

1. AVG

Op grond van artikel 5, eerste lid, aanhef en onder c, moeten persoonsgegevens die worden verwerkt toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (het beginsel van dataminimalisatie).

Daarnaast mogen persoonsgegevens op grond van artikel 6, vierde lid, AVG niet verder worden verwerkt als de verdere verwerking niet verenigbaar is met het doel waarvoor de persoonsgegevens zijn verzameld.

Dat betekent dat een aanbieder van gegevens bij iedere verstrekking/terbeschikkingstelling van persoonsgegevens moet nagaan of die zogenoemde verdere verwerking verenigbaar is met de doeleinden waarvoor de persoonsgegevens aanvankelijk zijn verkregen. De afnemer zal alleen die persoonsgegevens mogen verwerken die noodzakelijk zijn voor de doeleinden waarvoor hij de persoonsgegevens verwerkt.

Daarbij kan worden gedacht aan het (zoveel mogelijk) attesteren van stellingen in plaats van het verstrekken van documenten.

5.7 Het voorkomen van druk op het (digitaal) delen van gegevens

Een van de aspecten van de principes Mens Centraal en Balans in Belangen is dat een burger zich niet onder druk gezet mag voelen. Dat kan zowel druk betreffen om gebruik te maken van een bepaald systeem/een bepaalde regietoepassing, als druk om bepaalde gegevens te delen. Dat doet de vraag rijzen welke regels in het kader kunnen worden neergelegd om te voorkomen dat een burger dergelijke druk ervaart.

Vraagstuk 1: druk ten aanzien van het delen van gegevens

Afspraak/spelregel 1 met betrekking tot druk ten aanzien van het delen van gegevens:

Het delen van gegevens mag nooit worden beloond, in welke vorm dan ook.

Voorkomen moet worden dat een burger onder druk wordt gezet meer gegevens te delen dan noodzakelijk is voor de te leveren dienst. Een bekend voorbeeld is de burger die door een verzekeraar onder druk wordt gezet om aanvullende medische gegevens te delen en in ruil voor korting op de zorgpremie. Als regel zou kunnen worden voorgeschreven dat binnen een regietoepassing het delen van meer gegevens dan noodzakelijk voor de te leveren dienst *nooit* mag worden beloond, zowel niet met geld/kortingen, als met andere voordelen (vrijkaartjes, extra *features*, etc.). Ook mogen partijen met hun regietoepassing niet faciliteren dat burgers onder druk worden gezet.

Onderbouwing

1. AVG

Een van de grondslagen voor het verwerken van persoonsgegevens is de toestemming van de burger (artikel 6, eerste lid, aanhef en onder a, AVG). Van rechtsgeldige toestemming in de zin van de AVG is sprake indien de toestemming van de burger 1) vrijelijk, 2) specifiek, 3) geïnformeerd en 4) op een ondubbelzinnige wijze is verkregen.

De voorwaarde dat toestemming in de zin van de AVG vrijelijk moet worden gegeven, raakt aan het vraagstuk van het delen van gegevens onder druk. Deze voorwaarde houdt in dat de burger daadwerkelijk een vrije keuze moet hebben of hij toestemming geeft voor de verwerking van zijn persoonsgegevens. Een belangrijke voorwaarde daarbij is dat de burger geen nadelige gevolgen ondervindt indien hij zijn toestemming

weigert of intrekt. Zie daarover ook overweging 42 van de AVG en de *guidelines* van de Artikel 29 Werkgroep.[13]

2. Patiëntengeheim

Binnen het Ministerie van VWS wordt nagedacht over het voorkomen van delen onder druk in het kader van het patiëntengeheim. Een onderdeel van dat patiëntengeheim is een verbod op het onder druk zetten van een zorggebruiker om medische gegevens te delen, met inbegrip van een systeem van toezicht en handhaving.

(Beleids)vraag voor de toekomst: is het wenselijk aanvullende maatregelen te treffen om misleiding met betrekking tot het delen van gegevens te voorkomen, bijvoorbeeld zoals dat in het consumentenrecht is neergelegd, maar ook door middel van bewustwordingscampagnes?

Afspraak/spelregel 2 over de verhouding tussen toestemming en (de hoeveelheid) te gebruiken gegevens:

Van een burger verkregen toestemming doet niet af aan de proportionaliteits- en subsidiariteitsafweging die partijen moeten maken bij iedere gegevensverwerking.

Deze spelregel benadrukt dat een verkregen toestemming geen vrijbrief voor partijen kan opleveren om onder de noemer van verkregen toestemming ongelimiteerd gegevens te delen.

Onderbouwing

1. AVG

Op grond van artikel 5, eerste lid, aanhef en onder c, moeten persoonsgegevens die worden verwerkt toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (het beginsel van dataminimalisatie).

[13] Artikel 29 Werkgroep, 'Guidelines on consent under Regulation 2016/679', WP259 rev. 01, 10 april 2018, p. 5-6.

(Beleids)vraag voor de toekomst: wil je (los van juridische verplichtingen) regelen dat aanbieders, ook bij toestemming van een burger, steeds tot een bepaalde hoogte moeten beoordelen voor welk doel de gegevens worden gevraagd, en of dat een gerechtvaardigd doel is gelet op de aard en de hoeveelheid gegevens die worden gevraagd? En wil je daarbij bijvoorbeeld onderscheid maken tussen de afweging die aanbieders moeten maken bij een verstrekking aan publieke afnemers en de afweging die aanbieders moeten maken bij een verstrekking aan commerciële afnemers?

Vraagstuk 2: druk ten aanzien van het gebruik van een (digitale) regietoepassing

Afspraak/spelregel 1 voor analoge alternatieven:

De afnemer die een dienst verleent moet altijd zorgen dat de dienst ook analoog kan worden afgenomen.

Een burger kan niet worden verplicht gebruik te maken van een bepaalde digitale regietoepassing, althans niet als het gaat om overheidsdienstverlening. De mogelijkheid om dienstverlening niet via digitale weg te hoeven regelen en ontvangen, moet voor iedere burger blijven bestaan.

Onderbouwing

1. Wet elektronisch bestuurlijk verkeer (Webv)

Met de Webv is afdeling 2.3 toegevoegd aan de Algemene wet bestuursrecht (Awb). Deze afdeling bevat algemene regels over het elektronisch verkeer tussen burgers en bestuursorganen. Uit artikel 2:14 Awb volgt dat een bestuursorgaan berichten alleen elektronisch aan geadresseerden kan zenden voor zover een geadresseerde kenbaar heeft gemaakt dat hij langs elektronische weg voldoende bereikbaar is. Daarnaast mag een bericht nooit uitsluitend via de elektronische weg worden verzonden, tenzij bij wettelijk voorschrift is bepaald dat dit wel mag. Ook moeten berichten op een voldoende betrouwbare en vertrouwelijke manier worden verzonden.

Uit deze bepalingen volgt dat een bestuursorgaan niet zomaar berichten via elektronische weg aan een burger kan sturen. In de regel moet 1) de burger hebben aangegeven via die weg beschikbaar te zijn en 2) het bericht ook via andere (analoge)

weg worden gezonden, tenzij bij wettelijk voorschrift anders is bepaald (zoals bijvoorbeeld bij de Berichtenbox van MijnOverheid).

Overigens is er op dit moment een wetsvoorstel aanhangig om de bepalingen over elektronisch bestuurlijk verkeer te moderniseren.[14]

Let op: deze regels gelden alleen voor het verkeer tussen burgers en *bestuursorganen*.

2. Rapporten van de Nationale ombudsman

De Nationale ombudsman maakt zich al tijden hard voor de groep burgers die niet digitaal vaardig is en moeilijk of niet kan meekomen als het gaat om digitale communicatie met en door de overheid. In rapporten over onder meer de Dienst Uitvoering Onderwijs,[15] de Berichtenbox op MijnOverheid[16] en de Belastingdienst[17] heeft de Nationale ombudsman steeds benadrukt dat burgers zich niet gedwongen mogen voelen om gebruik te maken van een digitaal kanaal als zij dat niet willen of kunnen. Zij moeten de mogelijkheid hebben om overheidsberichten op papier te ontvangen.

De Nationale ombudsman heeft in 2017 een Ombudsvisie op digitalisering ontwikkeld, waarin hij aanbevelingen doet voor de digitale overheid. Daarin heeft de Nationale ombudsman vier uitgangspunten geformuleerd voor de overheid die digitaliseert:

- "**Neem verantwoordelijkheid**. De overheid is verantwoordelijk voor de inrichting en uitvoering van het dienstverleningsproces en neemt ook die verantwoordelijkheid;
- **Wees toegankelijk.** De overheid dient zijn infrastructuur (digitaal en niet-digitaal) zo in te richten dat de toegang tot die overheid voor iedere burger gewaarborgd is;
- **Wees oplossingsgericht.** De overheid zorgt ervoor dat fouten in het digitale systeem opgelost worden;
- **Wees gebruiksvriendelijk.** De overheid zet digitalisering in het belang van de gebruikers in en niet alleen vanuit het gemak voor de overheid; En laat goede dienstverlening daarbij het uitgangspunt zijn."[18]

Hoewel ook de Ombudsvisie alleen betrekking heeft op de overheid, en niet ook op private initiatieven om dienstverlening te digitaliseren, zou als afspraak/spelregel in het kader kunnen worden opgenomen dat bij alle dienstverlening de mogelijkheid moet blijven bestaan om die dienstverlening niet via de digitale weg te hoeven regelen en ontvangen.

[14] Zie voor dit wetsvoorstel: *Kamerstukken II* 2018/19, 35 218, nr. 2.
[15] No. 27 maart 2017, nr. 2017/040.
[16] No. 6 september 2017, nr. 2017/098.
[17] No. 5 april 2016, nr. 2016/030.
[18] www.nationaleombudsman.nl/nieuws/onderzoeken/ombudsvisie-op-digitalisering-overheid.

Afspraak/spelregel 2: het gebruik maken van het digitale systeem/de digitale regietoepassing mag niet worden beloond

Zie voor de onderbouwing afspraak/spelregel 1 van het vraagstuk druk ten aanzien van het delen van gegevens

Afspraak/spelregel 3 over recht op menselijke tussenkomst:

Iedere burger heeft recht op menselijke tussenkomst.

Uitgangspunt van regie op gegevens is dat de leefwereld leidend is boven de systeemwereld. De met digitalisering gepaard gaande standaardisatie kan ertoe leiden dat fouten kunnen worden gemaakt, doordat in de systeemwereld vaak niet op voorhand rekening kan worden gehouden met alle relevante aspecten van de – vele malen complexere – leefwereld. Hierom is het van belang dat de burger bij iedere regietoepassing de mogelijkheid heeft zich zo nodig tot een (menselijk) loket te wenden.

Om het recht op menselijke tussenkomst te garanderen, en te voorkomen dat de voordelen van digitalisering teniet worden gedaan, zou een sectoraal afsprakenstelsel of regietoepassing ervoor kunnen kiezen een burger inzicht en inzage te geven in de verschillende stappen van het gedigitaliseerde proces en per deelstap een correctie-/inputknop in te bouwen om deze rechten uit te oefenen en fouten te signaleren. De gegevensstroom kan op deze wijze gedigitaliseerd blijven verlopen, terwijl het recht op menselijke tussenkomst niet wezenlijk wordt aangetast. De geboden transparante en het enkele feit dát menselijke tussenkomst mogelijk is, zal de burger ook meer vertrouwen geven in het digitaliseerde proces.

Onderbouwing

1. Awb

In de Awb wordt de besluitvorming tot op zekere hoogte van menselijke tussenkomst voorzien door de hoorplichten en door de volledige heroverweging in de bezwaarfase.

2. AVG

In de AVG is al een recht op menselijke tussenkomst opgenomen. Artikel 22, derde lid, AVG stelt als voorwaarde voor volledig geautomatiseerde besluitvorming dat de burger het recht heeft op menselijke tussenkomst van de verantwoordelijke en dat hij zijn

standpunt kenbaar kan maken en het besluit kan aanvechten. De menselijke rol moet 'betekenisvol' zijn. De beslisser moet de mogelijkheid en autoriteit hebben om de automatische beslissing te wijzigen.

3. Advies van de Raad van State over de effecten van de digitalisering voor de rechtsstatelijke verhoudingen

De Raad van State spreekt in een ongevraagd advies over (kort gezegd) de effecten van digitalisering van de overheid over de noodzaak van zinvol contact met die overheid. Dat zinvolle contact kan er volgens de Raad van State aan in de weg staan dat er uitsluitend digitaal wordt gecommuniceerd.[19]

[19] Ongevraagd advies van de Raad van State over de effecten van de digitalisering voor de rechtsstatelijke verhoudingen, W04.18.0230/I, 31 augustus 2018; *Kamerstukken II* 2017/18, 26643, nr. 557.

5.8 Betalen voor gegevens

Vraagstuk: kunnen burgers worden verplicht te betalen voor hun gegevens?

Afspraak/spelregel voor het betalen voor gegevens:

Het in rekening brengen van vergoedingen mag er niet toe leiden dat een burger moet betalen voor gegevens waar hij kosteloos recht op heeft.

Bij (met name) bronhouders speelt de vraag of het mogelijk is vergoedingen in rekening te brengen voor de beschikbaarstelling van gegevens. In sommige gevallen kan dat. Een begrenzing is evenwel dat als een burger recht heeft op het kosteloos verkrijgen van bepaalde gegevens, hij niet vanwege gebruikmaking van een regietoepassing verplicht kan worden een vergoeding te betalen voor het verkrijgen van diezelfde gegevens.

Onderbouwing

1. AVG

In de AVG is bepaald dat een burger het recht heeft om van de verwerkingsverantwoordelijke *kosteloos* uitsluitsel te verkrijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en, wanneer zijn gegevens worden verwerkt, recht op een kopie van zijn gegevens. (artikel 12, vijfde lid AVG jo. artikel 15, derde lid AVG)

5.9 Tot slot: kluis versus sluis

Een terugkerende, meer algemene discussie binnen regie op gegevens is de vraag naar de wenselijkheid van kluistoepassingen ten opzichte van sluistoepassingen.[20] Bij sluistoepassingen is – kort gezegd – het idee dat een aanbieder op verzoek van een burger gegevens deelt met een afnemer. Dat verzoek van een burger zou kunnen worden begrepen als toestemming van de burger om gegevens te delen. Bij het delen van gegevens door een aanbieder op basis van deze toestemming gelden twee belangrijke kanttekeningen:

1) De toestemming van een burger vormt geen vrijbrief om ongelimiteerd gegevens te delen. Aanbieders zullen nog steeds moeten nagaan of zij een grondslag hebben voor de verstrekking en, in het verlengde daarvan, een proportionaliteits- en subsidiariteitsafweging moeten maken.

2) Sommige sectorale wet- en regelgeving bevat een gesloten verstrekkingsregime dat niet kan worden doorbroken door toestemming van de burger. Een voorbeeld is de Wet basisregistratie personen of (de geheimhoudingsplicht van) de Algemene wet inzake rijksbelastingen. De wet verbiedt dan het verstrekken van gegevens louter op basis toestemming. De ratio van een gesloten verstrekkingsregime is veelal juist bescherming van de burger. Indien de wens bestaat dit uitgangspunt los te laten, zal moeten worden gekeken in hoeverre dat moet leiden tot aanpassing van dit uitgangspunt. Conclusie kan ook zijn dat het niet wenselijk is het gesloten verstrekkingsregime te doorbreken en dus sluistoepassingen niet mogelijk zijn.

Kluistoepassingen zijn dan wellicht wel mogelijk. Daarvoor zal wel een voldoende stevige en specifieke wettelijke basis nodig zijn. Het structureel en/of op grote schaal verstrekken van persoonsgegevens door een aanbieder via een burger ten behoeve van regie op gegevens middels het inzagerecht van de AVG, lijkt oneigenlijk gebruik van dit recht.

[20] Voor een uitgebreidere beschrijving van deze verschillende toepassingen wordt verwezen naar het Kader voor Regie op gegevens en meer in het bijzonder het document 'Context en duiding'.

6 Bijlage

- Flowchart "Regie op gegevens – Ontwikkelen in lijn met de AVG"