Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

34 972 Algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur (Wet digitale overheid)

Nr. 4

ADVIES AFDELING ADVISERING RAAD VAN STATE EN NADER RAPPORT

Hieronder zijn opgenomen het advies van de Afdeling advisering van de Raad van State d.d. 3 mei 2018 en het nader rapport d.d. 12 juni 2018, aangeboden aan de Koning door de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties. Het advies van de Afdeling advisering van de Raad van State is cursief afgedrukt.

Bij Kabinetsmissive van 21 december 2017, no.2017002224, heeft Uwe Majesteit, op voordracht van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, bij de Afdeling advisering van de Raad van State ter overweging aanhangig gemaakt het voorstel van wet houdende regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur (Wet digitale overheid), met memorie van toelichting.

Samenleving en overheid digitaliseren. Dit vereist regels over wat wordt genoemd de (generieke) digitale infrastructuur.[1] Dit wetsvoorstel geeft regels voor de meest urgente onderdelen daarvan: elektronisch verkeer van en met de overheid (inbegrepen elektronische identificatiemiddelen), informatieveiligheid, toegang tot publieke dienstverlening voor burgers, en verantwoordelijkheidsverdeling voor infrastructuur en voorzieningen.

De Afdeling advisering van de Raad van State onderschrijft ten volle de noodzaak om op de kortst mogelijke termijn burgers, bedrijven en overheidsorganisaties elektronische identificatiemiddelen op een hoog beveiligd niveau te verschaffen. Betrouwbare toegang van burgers tot de overheid («inloggen») en tot publieke voorzieningen (zorg, onderwijs, werk en inkomen, persoonsregistraties, enzovoorts) en het veilig en ongestoord functioneren van overheidsorganisaties zijn hiervan afhankelijk. Daartoe is standaardisatie in de generieke digitale infrastructuur die overheidsorganisaties gebruiken een noodzakelijke voorwaarde. Om deze

[1] De generieke digitale infrastructuur bestaat uit standaarden, producten en digitale basisvoorzieningen die gezamenlijk gebruikt worden door overheden, publieke organisaties en in een aantal gevallen ook private partijen. Hierdoor is het mogelijk om primaire processen doelmatig in te richten en te blijven ontwikkelen.

kst-34972-4
ISSN 0921 - 7371
's-Gravenhage 2018

voorwaarde te realiseren moet één verantwoordelijk bewindspersoon deze technische standaarden vaststellen en aan overheidsorganen (centraal en decentraal) dwingend kunnen voorschrijven, met bevoegdheden van toezicht en ingrijpen. Het wetsvoorstel regelt zulks op zijn best halfslachtig. Dat is onwerkbaar[2] en gegeven het cruciale belang van standaardisatie niet verantwoord.

Met het oog op toegang van de burger tot de overheid, stelt het wetsvoorstel niet alleen regels voor publieke identificatiemiddelen maar ook voor private. De Afdeling onderschrijft dat een stelsel van private naast publieke middelen nuttig is. Toegang van burgers tot de overheid is een basisrecht dat evenwel niet afhankelijk mag worden van private partijen. Dit uitgangspunt is niet onomwonden en consequent in het wetsvoorstel neergelegd; daarnaast is de precieze verhouding tussen publieke en private middelen onvoldoende inzichtelijk vormgegeven en toegelicht.
De Afdeling advisering van de Raad van State adviseert dit wetsvoorstel pas naar de Tweede Kamer te sturen nadat het op genoemde punten wezenlijk is aangepast.

Blijkens de mededeling van de Directeur van Uw kabinet van 21 december 2017, no. 2017002224, machtigde Uwe Majesteit de Afdeling advisering van de Raad van State haar advies inzake het bovenvermelde voorstel van wet rechtstreeks aan mij te doen toekomen. Dit advies, gedateerd 3 mei 2018, nr. W04.17.0400/I, bied ik u hierbij aan.

1. Verantwoordelijkheid voor het stelsel als geheel

Het wetsvoorstel definieert en reguleert een deel van de generieke digitale infrastructuur: een stelsel dat burgers en bedrijven in staat stelt zich te identificeren[3] om toegang te krijgen tot elektronische diensten van de overheid of van «aangewezen organisaties» van buiten de overheid (zoals pensioenfondsen, zorgverleners, zorgverzekeraars en instellingen voor hoger onderwijs). Het stelsel wordt bij en krachtens[4] de wet ingesteld en vormgegeven; de Minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) krijgt een zorgplicht voor het inrichten en in stand houden van het stelsel.[5]
Het wetsvoorstel vormt de eerste tranche van de Wet digitale overheid. Het regelt de meest urgente onderwerpen en biedt de basis voor verdere uitbreiding en modernisering, maar gaat daar overigens in de toelichting niet nader op in.

Deze generieke digitale infrastructuur is organisatorisch complex: het stelsel wordt gebruikt door honderden bestuursorganen (zoals provincies, gemeenten en zelfstandige bestuursorganen), rechterlijke organen en door organisaties buiten de overheid. Aan al deze bestuursorganen en organisaties worden in het wetsvoorstel eisen gesteld.

---

[2] Belangrijke redenen dat grote ICT projecten in de overheid vastlopen, zoals recent de Basisregistratie personen en het KEI-project voor de rechtspraak, zijn het gebrek aan daadwerkelijke standaardisatie en aan éénduidige sturing. Rapport van de commissie Parlementair onderzoek naar ICT-projecten bij de overheid (commissie-Elias), Kamerstukken II 2014/15, 33 326, nr. 5, blz. 72–73.

[3] Het voorstel maakt onderscheid tussen identificatie (opgeven van de identiteit) en authenticatie (controleren van de juistheid van de opgegeven identiteit). De vragen in dit advies gaan over identificatie, huiselijk verwoord als «inloggen».

[4] Artikel 3; bij algemene maatregel van bestuur worden nadere regels gesteld over standaarden en het functionele toepassingsbereik.

[5] Artikel 5.

– *Zij worden verplicht om alle inlogmiddelen die door de Minister van BZK zijn toegelaten (naast het bekende DigiD en varianten daarvan ook een of meer private inlogmiddelen) te accepteren.*[6]
– *Zij moeten ervoor zorgen dat de toegang tot hun elektronische diensten goed werkt en betrouwbaar en veilig is; zij rapporteren daarover aan de Minister.*[7] *Zij moeten tevens bepalen voor welke diensten zij authenticatie op een bepaald betrouwbaarheidsniveau gaan voorschrijven.*[8]
– *Zodra Nederland zijn eigen stelsel voor identificatiemiddelen heeft aangemeld bij de Europese Commissie moeten bestuursorganen ook alle buitenlandse identificatiemiddelen die bij de Commissie zijn aangemeld accepteren.*

De generieke digitale infrastructuur beoogt burgers en bedrijven in staat te stellen op een veilige en gebruikersvriendelijke manier elektronisch contact te onderhouden met de overheid. Burgers hebben zelden goed zicht op het grote aantal organisaties waarover de overheidstaak is verdeeld en op die taakverdeling. Het is voor hen moeilijk te begrijpen en te hanteren wanneer elke organisatie, belast met een deel van de overheidstaak, de digitale communicatie met burgers in een ander tempo en op een andere manier aanpakt.

Dit burgerperspectief betekent dat de organisaties die worden aangesloten op de generieke digitale infrastructuur hun communicatie op een gestandaardiseerde en voorspelbare manier dienen aan te bieden; en dat de invoering en modernisering van de elektronische communicatie niet teveel in de tijd moet uiteenlopen. Het belang van standaardisatie en synchronisatie speelt niet alleen bij deze eerste tranche, maar is ook van belang bij volgende tranches van de Wet digitale overheid.

De Afdeling acht het dan ook van belang dat de Minister van BZK over voldoende bevoegdheden beschikt om de standaardisatie in technisch opzicht en de synchronisatie van dit proces daadwerkelijk te kunnen realiseren – niet alleen op basis van dit voorstel, maar ook voor de verdere uitbouw van de digitale overheidscommunicatie. Standaardisatie gaat immers niet vanzelf.

Vanuit dit belang en perspectief acht de Afdeling het wetsvoorstel op de navolgende onderdelen onvoldoende.[9]
– *Bevoegdheden. De verhouding tussen de Minister die verantwoordelijk is voor het beheer van de generieke digitale infrastructuur en andere Ministers, bestuursorganen en andere overheden is op het punt van de technische standaardisatie onduidelijk. De Minister «bevordert» de interoperabiliteit tussen infrastructuren, diensten en organisaties,*[10] *maar kan deze niet dwingend voorschrijven. Zo ontbreekt in het voorstel een bevoegdheid om besluiten van overheidsorganisaties over standaarden en andere technische specificaties die een snelle en betrouwbare aansluiting op de generieke digitale infrastructuur in de weg staan te schorsen of te vernietigen, alsmede een bevoegdheid om op deze punten bindende aanwijzingen te geven en zo nodig in laatste instantie werkzaamheden zelf te doen uitvoeren, op kosten van de betreffende organisatie.*

---

[6] Artikelen 7, eerste lid, en 13, tweede lid.
[7] Artikel 4.
[8] Artikel 6, tweede lid.
[9] Onverlet artikel 3, tweede en derde lid. De bepaling dat bij algemene maatregel van bestuur standaarden kunnen worden aangewezen en bepaald, neemt de kanttekeningen bij de hierna genoemde onderdelen niet weg. Die bevoegdheid is immers beperkt tot het aanwijzen van open standaarden voor software.
[10] Artikel 5.

– *Bestuurlijk toezicht.[11] De Minister van BZK krijgt geen bijzondere toezichtsbevoegdheden. Volgens de toelichting geldt het reguliere toezicht (aangevuld met een jaarlijkse audit, uit te brengen aan de Minister). Meer concreet: elke vakminister oefent toezicht uit op de eigen uitvoeringsorganisaties, en op de zelfstandige bestuursorganen en de aangewezen organisaties die op zijn beleidsterrein liggen. En: decentrale overheden zijn zelf verantwoordelijk voor de naleving van de wet. De Minister heeft alleen de bevoegdheden van het zogenoemde generiek interbestuurlijk toezicht: van rijk op provincies, van provincies op gemeenten. Dat toezicht is bedoeld als sober en terughoudend en in hoofdzaak gericht op bestuurlijke en financiële verhoudingen. Het is bedoeld noch ingericht voor technische, organisatorische en uitvoerende kwesties, zoals die zich voordoen in de digitale (overheids-)infrastructuur. De vormgeving van het bestuurlijk toezicht moet om die reden opnieuw worden doordacht en het voorstel moet vervolgens worden aangepast.*
– *Toezicht op naleving van voorschriften. Het voorstel maakt het mogelijk om toezichthouders aan te wijzen, die de beschikking krijgen over de klassieke toezichtsbevoegdheden. Zo kunnen zij plaatsen betreden, inzage vorderen van zakelijke gegevens en bescheiden, zaken onderzoeken en daarvan monsters nemen. Zij kunnen toezicht houden op organisaties die zijn aangesloten op de generieke digitale infrastructuur, op bedrijven die private identificatiemiddelen verschaffen en op bedrijven die worden ingeschakeld bij de identificatie.[12] Deze fysieke vorm van toezicht past niet goed in de verhouding met bestuursorganen. Waar het gaat om toezicht op genoemde bedrijven is dat wel voorstelbaar. Het valt echter op dat geen bevoegdheden worden toegekend die toegesneden zijn op een digitaal stelsel, zoals toegang tot geautomatiseerde programma's en gegevens. Het voorstel verdient nadere uitwerking en toelichting, met daarbij jegens bedrijven als uitgangspunt dat er een passend instrumentarium moet zijn om te kunnen ingrijpen, vergezeld van passende waarborgen.*
– *Calamiteiten. Bij een ernstige storing of ernstige aantasting van de werking, beveiliging of betrouwbaarheid van de elektronische dienstverlening, of bij misbruik of oneigenlijk gebruikt van de toegang tot elektronische dienstverlening, kan de Minister de toegang tot elektronische dienstverlening van een bestuursorgaan of aangewezen organisatie onderbreken.[13] Het valt op dat de Minister pas kan ingrijpen wanneer een storing of aantasting zich al voordoet, en niet al bij een ernstige dreiging daarvan. Verder is de samenhang met andere wetgeving van belang. In het voorstel van een Cybersecuritywet, waarin de EU-richtlijn over beveiliging van netwerk- en informatiesystemen wordt geïmplementeerd, worden instanties aangewezen met een coördinerende taak bij het beveiligen van vitale infrastructuren («bevoegde autoriteiten»). De Minister van Economische Zaken en Klimaat wordt aangewezen als bevoegde autoriteit voor de digitale infrastructuur.[14] Ook in het stelsel van de Telecommunicatiewet komen noodbevoegdheden (bevoegdheden die alleen toegepast mogen worden onder buitengewone omstandigheden) toe aan de Minister van Economische Zaken en Klimaat.[15] Dit roept de vraag op waarom de Minister van BZK geen bijzondere bevoegdheden heeft voor het overheidsgedeelte van de digitale infrastructuur, dat onderwerp is van het voorliggende wetsvoorstel.*

---

[11] Artikel 15.
[12] Artikel 15 in combinatie met titel 5.2 van de Algemene wet bestuursrecht.
[13] Artikel 16.
[14] Artikel 4, eerste lid, van het voorstel van een Cybersecuritywet, Kamerstukken II 2017/18, 34 883, nr. 2.
[15] Hoofdstuk 14 van de Telecommunicatiewet.

– *Identiteitsfraude. In de toelichting wordt terecht ingegaan op de groei van het probleem van identiteitsfraude.*[16] *Dit probleem hangt nauw samen met de uitgifte van identificatiemiddelen, maar ook met het inloggen met zulke middelen bij de overheid. De Minister krijgt de plicht om maatregelen te treffen bij een vermoeden van misbruik van een identificatiemiddel.*[17] *Wat in het voorstel ontbreekt is een duidelijk belegde verantwoordelijkheid voor het oplossen van de problemen waar slachtoffers van identiteitsfraude mee te maken krijgen. Zo is niet geregeld welk orgaan daarvoor verantwoordelijk is, waar het slachtoffer zich kan melden en hoe hij op een eenvoudige manier een identificatiemiddel tijdelijk kan onderbreken, bijvoorbeeld bij zoekgeraakte of gestolen documenten.*[18]

De Afdeling adviseert het voorstel aan te passen aan de hand van de hiervoor genoemde punten.

1. Verantwoordelijkheid voor het stelsel als geheel

Inzake de verantwoordelijkheid voor het stelsel als geheel wijst de Afdeling, vanuit het burgerperspectief, op het belang van standaardisatie en synchronisatie van bij de generieke digitale infrastructuur (hierna: gdi) aangesloten (overheids)organisaties, bij deze en volgende tranches van de Wet digitale overheid. De Afdeling acht het daarom van belang dat de Minister van BZK over voldoende bevoegdheden beschikt om de standaardisatie in technisch opzicht en de synchronisatie van dit proces ook daadwerkelijk te kunnen realiseren. In dat verband doet de Afdeling een aantal aanbevelingen.

In de eerste plaats zou in het wetsvoorstel een bevoegdheid moeten worden opgenomen om besluiten van overheidsorganisaties over standaarden en andere technische specificaties die een snelle en betrouwbare aansluiting op de gdi in de weg staan te schorsen of te vernietigen, alsmede een bevoegdheid om op deze punten bindende aanwijzingen te geven en zo nodig werkzaamheden zelf te doen uitvoeren op kosten van de betreffende organisatie.
In reactie hierop wordt opgemerkt dat, mede gelet op de verantwoordelijkheid van de Minister van BZK voor de gdi, hij ingevolge artikel 3 van het wetsvoorstel bij algemene maatregel van bestuur (technische) standaarden kan voorschrijven teneinde interoperabiliteit te bewerkstelligen. In aansluiting op het advies van de Afdeling is het afdwingen van daadwerkelijke toepassing van de voorgeschreven standaarden nader gereguleerd. Artikel 3 is aangevuld met de bevoegdheid voor de Minister van BZK om (bindende) aanwijzingen te geven aan overheden en organisaties die concurrerende (dat wil zeggen met ingevolge artikel 3 vastgestelde interfererende) open standaarden hanteren. Tevens is voorzien in de mogelijkheid om inzake de aanwijzing van standaarden nadere regels te stellen, waaronder de mogelijkheid om de toepassing van de voorgeschreven standaarden aan een periodieke audit te onderwerpen en regels te stellen over het rapporteren van bevindingen terzake. Vanuit het burgerperspectief is het van belang er op te wijzen, dat wanneer een voorgeschreven standaard niet wordt toegepast, deze – gerelateerd aan een besluit of feitelijk handelen – in rechte kan worden ingeroepen jegens de desbetreffende overheidsorganisatie. Voor een succesvol beroep door een burger of bedrijf op een onrechtmatige overheidsdaad (artikelen 6:162–163 BW) zijn toerekenbaarheid, relativiteit

[16] Toelichting, paragraaf 5.2 (Aanpak van misbruik en identiteitsfraude).
[17] Artikel 16, vierde lid.
[18] Advies van de commissie evaluatie pilots publieke en private authenticatiemiddelen (commissie-Kuipers), 31 mei 2016, Kamerstukken II 2015/16, 26 643, nr. 419, bijlage, blz. 30.

(strekt de standaard mede tot bescherming van het belang van burgers en bedrijven), aantoonbare schade en causaliteit vereist.

Voorts adviseert de Afdeling de vormgeving van het bestuurlijk toezicht nogmaals te doordenken en de Minister van BZK in dit verband passende bevoegdheden te geven. Het valt de Afdeling op dat geen bevoegdheden worden toegekend die toegesneden zijn op een digitaal stelsel, zoals toegang tot geautomatiseerde programma's en gegevens. De Afdeling adviseert het voorstel nader uit te werken en toe te lichten, met daarbij jegens bedrijven als uitgangspunt dat er een passend instrumentarium moet zijn om te kunnen ingrijpen, vergezeld van passende waarborgen.

In reactie hierop zij opgemerkt dat bestuursorganen en aangewezen organisaties, aanbieders van een toegelaten identificatiemiddel en op grond van artikel 11 erkende middelenuitgevers en diensten met het wetsvoorstel worden verplicht om mij desgevraagd en uit eigen beweging de gegevens en inlichtingen te verstrekken die ik nodig heb om maatregelen te kunnen nemen om inbreuk op de veilige en betrouwbare toegang tot elektronische dienstverlening te voorkomen of beëindigen. Bezien wordt of daarnaast de inzage in programmatuur een passend instrument is om te controleren of de aanbieder van een toegelaten privaat identificatiemiddel voldoet aan de terzake krachtens de eIDAS-verordening vastgestelde technische specificaties en procedures. Zo nodig wordt deze bevoegdheid deel van de overeenkomst die ik sluit als resultaat van de aanbesteding van een privaat authenticatiemiddel c.q. authenticatiedienst.

In reactie op het advies om de vormgeving van het bestuurlijk toezicht nogmaals te doordenken wordt opgemerkt, dat het wetsvoorstel op het gebied van toezicht op de naleving aansluit bij de bestaande systematiek, verantwoordelijkheidsverdeling en instrumenten. Daarnaast wordt inzake informatieveiligheid een auditplicht jegens de Minister van BZK ingevoerd en krijgt de Minister van BZK noodbevoegdheden bij (dreigende) calamiteiten. Dit samenstel van verantwoordelijkheden, taken en bevoegdheden maakt dat de effectiviteit van de regels inzake de toegang tot dienstverlening wordt versterkt en dat op dit punt nadere regulering voorshands (dat wil zeggen: tot aan de geplande evaluatie) niet opportuun is.

In aansluiting op de zienswijze van de Afdeling dat de verdere uitbouw van de digitale overheid noopt tot voldoende bevoegdheden van de Minister van BZK, wordt het volgende opgemerkt. De in artikel 5, eerste lid, van het wetsvoorstel opgenomen zorgplicht van de Minister van BZK omvat de inrichting, beschikbaarstelling, instandhouding, werking en beveiliging van de generieke digitale infrastructuur. Vervolgens reguleert het wetsvoorstel primair hetgeen nodig is in het kader van de toegang tot elektronische dienstverlening (eID). Zoals in de memorie van toelichting wordt opgemerkt, wordt beoogd in de toekomst meer generieke voorzieningen en functionaliteiten (dus: los van eID) onder het regime van de Wet digitale overheid te brengen indien dit, gezien hun aard en reikwijdte, nuttig en noodzakelijk is. Hiertoe kunnen te zijner tijd nieuwe tranches van de wet worden ingediend.
Om, aansluitend bij hetgeen de Afdeling adviseert, synchronisatie van dit proces daadwerkelijk en voortvarend te kunnen realiseren, passend bij de beleids- en systeemverantwoordelijkheid van de Minister van BZK, is het wetsvoorstel aangevuld. Er is een grondslag opgenomen voor het bij algemene maatregel van bestuur stellen van regels met het oog op de inrichting, beschikbaarstelling, instandhouding, werking en beveiliging van de generieke digitale infrastructuur, waaronder inzake andere gdi-voorzieningen en verplichte aansluiting hierop door – tevens bij amvb te bepalen – (overheids)organisaties. Hierdoor kan snel worden

ingespeeld op nieuwe ontwikkelingen. Indien deze uitvoeringsregels worden vastgesteld, worden ook de kosten samenhangend met de uitvoering doorberekend. Beoogd wordt de kosten voor het gebruik van de verplichte gdi-voorzieningen naar rato van gebruik door te belasten aan aangesloten organisaties. In het geval een organisatie, anders dan wordt voorgeschreven, geen gebruik maakt van de gdi-voorziening zal desalniettemin een forfaitair bedrag in rekening worden gebracht.

Voorts adviseert de Afdeling te voorzien in meer bevoegdheden voor de Minister van BZK bij calamiteiten. Anders dan de Afdeling veronderstelt, bevat het wetsvoorstel wel bijzondere bevoegdheden in relatie tot het overheidsgedeelte van de digitale infrastructuur, met als ultieme bevoegdheid het afsluiten van de toegang tot elektronische dienstverlening van een bestuursorgaan of aangewezen organisatie. Met de Afdeling ben ik van mening dat het wetsvoorstel verduidelijkt kan worden op het punt van bevoegdheden bij dreiging van een ernstige storing of aantasting (preventief optreden); het wetsvoorstel is op dit punt aangepast.

Tot slot adviseert de Afdeling de verantwoordelijkheid van de Minister van BZK voor de aanpak van identiteitsfraude te verankeren. Terecht wijst de Afdeling op de in het wetsvoorstel vervatte bevoegdheid van de Minister van BZK in het geval van (vermoed) misbruik van het identificatiemiddel. Met de Afdeling ben ik van mening dat de problemen, waar slachtoffers van identiteitsfraude mee te maken krijgen, aandacht behoeven. In dat verband zij gewezen op het Centraal Meldpunt Identiteitsfraude (CMI), onderdeel van mijn ministerie, dat advies en ondersteuning biedt aan slachtoffers van identiteitsfraude. Momenteel wordt door mij de opportuniteit van een wettelijke verankering van de rol van de Minister van BZK bij de aanpak van identiteitsfraude nader onderzocht. Gelet op de reikwijdte van het onderhavige wetsvoorstel en het feit, dat identiteitsfraude een complex geheel is en een bredere portee heeft dan digitale identificatie, ligt regulering in de Wet digitale overheid niet in de rede.

2. Publieke en private identificatiemiddelen

Het voorstel beoogt te regelen dat burgers, bedrijven en organisaties op een betrouwbare manier kunnen inloggen bij bestuursorganen en aangewezen organisaties (met name zorginstellingen, zorgverleners, instellingen voor hoger onderwijs en pensioenfondsen).

Voor burgers komen er door de overheid gecreëerde identificatiemiddelen op drie «betrouwbaarheidsniveaus» (deze betrouwbaarheidsniveaus – laag, substantieel en hoog – zijn gedefinieerd in de «eIDAS-verordening» van de Europese Unie).[19] Het huidige DigiD, dat al sinds 2005 in gebruik is, heeft betrouwbaarheidsniveau «laag». Het zal worden aangevuld met «Versterkt DigiD» op niveau «substantieel».[20] Verder komt er een identificatiemiddel via een chip op de identiteitskaart en het rijbewijs, op betrouwbaarheidsniveau «hoog». De burger betaalt voor de verstrekking van deze middelen leges.[21] Daarnaast komen er voor burgers private

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

[20] Artikel 3, derde lid, van de Regeling voorzieningen GDI. Bij het inloggen met DigiD wordt een extra controle uitgevoerd aan de hand van een niet-zichtbare chip in een bestaand paspoort, identiteitskaart of rijbewijs. De chip kan worden uitgelezen met een kaartlezer of met een smartphone. Nadere uitleg is te vinden in Stcrt. 2017, Nr. 59901, en in Evaluatierapport pilot DigiD-RDA, DigiD versterkt met controle van het identiteitsbewijs van de RDW, 23 mei 2016, Kamerstukken II 2015/16, 26 643, nr. 419, bijlage.

[21] Artikel 18.

identificatiemiddelen, die door de Minister van BZK worden toegelaten. De eIDAS-verordening biedt de mogelijkheid om zulke private middelen toe te laten (die dan moeten voldoen aan de betrouwbaarheidseisen van de verordening), maar verplicht daar niet toe.

Bedrijven en organisaties kunnen uitsluitend inloggen met een zogeheten bedrijfs- en organisatiemiddel, dat via publiek-private samenwerking is ontwikkeld en door de Minister van BZK wordt erkend.[22] De inlogmethode voor bedrijven en organisaties zal ook gelden voor overheidsorganisaties.

Een burger die, om toegang tot de overheid krijgen, een privaat identificatiemiddel gebruikt, bijvoorbeeld door het hanteren van een bankpas voorzien van een elektronische identificatie, moet zich realiseren dat hij daarmee juridisch gezien een overeenkomst afsluit met de onderneming die dat middel verschaft (in dit voorbeeld, zijn bank), de voorwaarden die die onderneming hanteert accepteert en voor deze dienstverlening betaalt.

Het voorstel kiest aldus voor een gemengd publiek en privaat stelsel. De Afdeling begrijpt de keuze om naast publieke, ook private identificatiemiddelen toe te staan. Economische ontwikkeling, innovatie en keuzevrijheid van burgers en bedrijven worden immers bevorderd indien het stelsel meerdere identificatiemiddelen toelaat. Het is bovendien van wezenlijk belang dat de eenzijdige afhankelijkheid van één middel in de digitale infrastructuur («single points of failure») wordt verkleind door voor eenzelfde doel, in dit geval identificatie en inloggen, meer middelen (instrumenten) beschikbaar te doen zijn. De Afdeling merkt evenwel op dat de vormgeving van een stelsel van private naast publieke middelen ook de navolgende vragen oproept die in het wetsvoorstel nadere toelichting of aanpassing behoeven.

- *Basisrecht. Toegang van burgers (en bedrijven) tot en communicatie met de overheid is een basisrecht, een publieke verantwoordelijkheid en mag niet afhankelijk worden van private partijen. Daarom moet de overheid zelf, met eigen middelen, waarborgen – niet alleen juridisch, maar ook feitelijk – dat burgers elektronische toegang tot de overheid hebben op een voldoende hoog betrouwbaarheidsniveau. Dit principiële uitgangspunt is in de toelichting bij het wetsvoorstel niet onomwonden verwoord en in het voorstel en de toelichting evenmin consequent doorgevoerd. Er is bijvoorbeeld een risico dat het toelaten van private middelen de invoering van publieke middelen op verschillende betrouwbaarheidsniveaus vertraagt of hindert; het Bureau ICT-toetsing heeft op dit risico gewezen.[23]*
- *Inloggen door de overheid bij de overheid. Het voorstel bepaalt dat overheidsorganisaties alleen met (private) bedrijfs- en organisatiemiddelen kunnen inloggen bij bestuursorganen als zij elkaar beveiligde gegevens willen toesturen (dat wil zeggen: als de gegevensuitwisseling plaatsvindt op betrouwbaarheidsniveau substantieel of hoog).[24] Het is de Afdeling niet duidelijk waarom vertrouwelijk gegevensverkeer tussen overheden onderling alleen mogelijk zou moeten zijn via private middelen. Het ligt juist meer in de rede dat de overheid door middel van door de overheid gecreëerde identificatiemiddelen zoveel mogelijk controle heeft over zulke gegevensuit-*

---

[22] Artikel 7, tweede lid, aanhef en onderdeel a, in combinatie met artikel 11, eerste lid. Zie ook de definities van «publiek identificatiemiddel» en «privaat identificatiemiddel» in artikel 1.

[23] Advies van 13 mei 2016, kenmerk 20 16–0000282302, blz. 6.

[24] Artikel 13, eerste lid, in combinatie met artikel 6, tweede lid, van de Handelsregisterwet 2007; toelichting op artikel 11. Zie ook de toelichting op artikel 13, waar gesteld wordt: «Bovendien mogen [bestuursorganen en aangewezen organisaties] uitsluitend toegang verlenen tot hun dienstverlening in geval gebruik wordt gemaakt van een erkend bedrijfs- en organisatiemiddel.»

wisseling om haar verantwoordelijkheid voor een veilig verloop te kunnen waarmaken.

– *Marktordening en gelijk speelveld. De Minister kan ingevolge dit wetsvoorstel[25] het gebruik van private identificatiemiddelen voor toegang tot de overheid toelaten. Hij bepaalt op dat moment hoeveel private middelen hij toelaat en de duur van de toelating.[26] Het wetsvoorstel gaat uit van een situatie van schaarste en kiest voor een stelsel met een vergelijkende toets op basis van vooraf bekendgemaakte criteria.[27] De veronderstelde schaarste en de keuze voor dit stelsel wordt slechts summier toegelicht. Er is met andere woorden niet gekozen voor een open stelsel, waarbij iedere aanbieder van een identificatiemiddel die aan bepaalde eisen voldoet tot de markt wordt toegelaten.[28] Bij de verdeling van schaarse rechten, het in het wetsvoorstel gekozen stelsel, dient evenwel een gelijk speelveld te bestaan. Dat houdt in dat een passende mate van openbaarheid moet zijn verzekerd over het aantal toelatingen en de duur daarvan, de selectieprocedure, het aanvraagtijdvak en de toe te passen criteria. De Minister moet hierover tijdig voorafgaand aan de start van de procedure duidelijkheid scheppen. Die duidelijkheid bevatten het wetsvoorstel en de toelichting nog niet. Er wordt in het wetsvoorstel evenmin bijzondere aandacht besteed aan (bestaande) private authenticatiediensten die ook gebruikt (kunnen) worden door burgers om zich te identificeren bij overheidsdiensten, en aan de vraag welke regels daarvoor (gaan) gelden dan wel hoe deze bestaande private authenticatiemiddelen zich (gaan) verhouden tot het in het wetsvoorstel beoogde stelsel van toelating van private middelen.*

De Afdeling adviseert de hiervoor genoemde punten nader te bezien en waar nodig het voorstel aan te passen.

2. Publieke en private identificatiemiddelen

Inzake publieke en private identificatiemiddelen heeft de Afdeling begrip voor de keuze voor een gemengd stelsel. Bij de voorgestelde vormgeving heeft de Afdeling een aantal vragen.

In de eerste plaats is de Afdeling van mening dat toegang van burgers (en bedrijven) tot en communicatie met de overheid een basisrecht en een publieke verantwoordelijkheid is, dat niet afhankelijk mag worden van private partijen. In reactie hierop zij er op gewezen dat voor burgers de overheid zelf middelen op diverse betrouwbaarheidsniveaus zal uitgeven, los van het eventueel toelaten van private middelen. Deze verantwoordelijkheid voor de invoering van publieke middelen is verankerd in artikel 5, eerste lid, onder a, juncto artikel 9, eerste lid, van het wetsvoorstel, waarin een zorgplicht voor de Minister van BZK is vervat. Dit is anders voor bedrijven, waar niet wordt voorzien in een publiek middel. Het stelsel terzake met louter private middelen (het huidige e-Herkenning) functioneert reeds jaren naar tevredenheid en zal, met het oog op de veiligheid en betrouwbaarheid, worden doorontwikkeld door marktpartijen. Nut en noodzaak van een publiek middel ontbreken hier. Met het onderhavige wetsvoorstel wordt het stelsel evenwel publiekrechtelijk ingekaderd. Dit betekent dat voor private middelen nodig is dat deze, teneinde toegang tot overheidsdienstverlening mogelijk te maken, erkend zijn door de Minister van BZK op basis van vooraf gesteld eisen.

---

[25] Artikel 9, tweede lid.
[26] Artikel 9, tweede en derde lid.
[27] Artikel 9, tweede lid, aanhef en onderdeel c.
[28] Toelichting op artikel 9, tweede lid.

Overigens ben ik met de Afdeling van mening dat er een recht op toegang tot en communicatie met de overheid bestaat. Bezien zal worden of en op welke wijze dit principiële uitgangspunt, dat een bredere werkingssfeer heeft dan het onderhavige wetsvoorstel, in de wetgeving kan worden opgenomen.

De Afdeling is voorts van mening dat inloggen door de overheid bij de overheid ook met publieke middelen zou moeten kunnen geschieden. In reactie hierop zij, onder verwijzing naar het voorgaande punt, opgemerkt dat het wetsvoorstel er in voorziet dat publieke middelen worden gebruikt door burgers (natuurlijke personen). Ondernemingen (bedrijven) en (publiekrechtelijke en privaatrechtelijke) rechtspersonen gebruiken private middelen. Er zijn voor rechtspersonen geen publieke middelen beschikbaar. Dat is ook niet problematisch, want de voor hen beschikbare private middelen moeten door de Minister van BZK erkend zijn. Hoewel niet van overheidswege uitgegeven, is er daarbij sprake van publiekrechtelijke inkadering. Het gegevensverkeer is, met het oog op betrouwbaarheid en veiligheid, ook bij het gebruik van erkende private middelen aan strenge eisen en toezicht onderworpen.

Tot slot adviseert de Afdeling duidelijkheid vooraf te scheppen waar het gaat om (het proces van) toelating van private identificatiemiddelen voor burgers alsmede aandacht te besteden aan de regels voor (bestaande) private authenticatiediensten die middelen voor burgers aanbieden. In reactie hierop wordt opgemerkt, dat transparantie wordt verschaft door het samenstel van het in artikel 9 van het wetsvoorstel bepaalde, de krachtens de eIDAS-verordening vastgestelde (toelatings)eisen, de vergelijkende toets en de hiertoe vooraf bekendgemaakte eisen en criteria (aanbesteding). In dit verband zij benadrukt dat bestaande private authenticatiediensten geen preferente positie hebben; zij moeten, om kans te maken op toelating van het door hen aangeboden middel, de door de Minister vastgestelde procedure doorlopen en bij de gunning uiteindelijk worden geselecteerd.

3. Gebruik Burgerservicenummer buiten de overheid

Het wetsvoorstel stelt regels voor elektronische dienstverlening door de overheid, maar is mede van toepassing op organisaties buiten de overheid die nu al gebruik maken van het Burgerservicenummer (BSN) en DigiD: instellingen voor hoger onderwijs, pensioenfondsen, zorgaanbieders en zorgverzekeraars. Ook andere organisaties die het BSN mogen gebruiken kunnen – bij algemene maatregel van bestuur of bij ministerieel besluit – onder het stelsel worden gebracht.[29] Zulke organisaties kunnen dan gebruik maken van het stelsel van publieke en private identificatiemiddelen, dat in het voorstel wordt neergezet. Zij worden dan aangesloten op de generieke digitale infrastructuur en komen onder het toezicht te staan van de Minister van BZK.[30]

De Wet algemene bepalingen burgerservicenummer bepaalt weliswaar dat organisaties buiten de overheid het BSN alleen mogen gebruiken als zij daar bij of krachtens de wet toestemming voor hebben gekregen, maar bevat zelf geen criteria. Het voorliggende wetsvoorstel bevat die criteria evenmin. Dat betekent dat de reikwijdte van het wetsvoorstel bij bijzondere wet kan worden uitgebreid en dat er geen algemene criteria

[29] Artikel 2.
[30] Artikel 15.

zijn om te bepalen welke organisaties daarvoor in aanmerking komen.[31] De Afdeling acht het van belang dat het gebruik van publieke identificatiemiddelen en het BSN alleen wordt uitgebreid tot organisaties buiten de overheid op basis van duidelijke, wettelijke criteria. Zij adviseert dergelijke criteria op te nemen in dit wetsvoorstel of in de Wet algemene bepalingen burgerservicenummer.

3. Gebruik Burgerservicenummer buiten de overheid

Inzake het gebruik van het burgerservicenummer (bsn) buiten de overheid adviseert de Afdeling, mede gelet op de koppeling tussen bsn gebruikende organisaties en de – in dit wetsvoorstel gereguleerde – toegang tot hun elektronische dienstverlening, wettelijke criteria te ontwikkelen voor het mogen gebruiken van bsn door organisaties buiten de overheid, zoals zorginstellingen. In reactie hierop zij opgemerkt dat de relevantie van dit punt wordt onderkend, maar dat dit buiten de werkingssfeer van het onderhavige wetsvoorstel valt. Immers, het wetsvoorstel haakt slechts aan bij organisaties die het bsn al mogen verwerken op grond van bestaande wetgeving. Bezien zal worden of het opportuun is om bij gelegenheid de Wet algemene bepalingen burgerservicenummer aan te passen.

4. Bescherming van persoonsgegevens

Het wetsvoorstel brengt met zich mee dat een groot aantal persoonsgegevens op diverse plaatsen zal worden verwerkt. De bevoegdheid om persoonsgegevens, waaronder het BSN, te verwerken wordt toegekend aan de Minister van BZK, bestuursorganen, aangewezen organisaties, uitgevers van private identificatiemiddelen en erkende diensten die betrokken zijn bij authenticatie. De enige beperking aan deze verwerkingsbevoegdheid is dat verwerking noodzakelijk moet zijn voor de uitvoering van de wet of voor de werking van het identificatiemiddel. Bij algemene maatregel van bestuur worden nadere regels gesteld.[32] De Afdeling heeft twee aandachtspunten.

a. Daadwerkelijke bescherming

De Afdeling constateert dat de toelichting op het wetsvoorstel terecht uitgebreid en adequaat ingaat op de verhouding met de Algemene Verordening Gegevensbescherming (AVG).[33] Daarbij is van belang dat de AVG, anders dan de privacyrichtlijn[34], een verordening is die rechtstreekse werking in de Nederlandse rechtsorde heeft. Dit brengt met zich dat de wetgever slechts ruimte heeft om nadere regels te stellen voor zover de AVG dat uitdrukkelijk toelaat. De vraag is daarom in hoeverre er onder het regime van de AVG nog bevoegdheid is om bij algemene maatregel van bestuur nadere regels te stellen voor de afzonderlijke in de toelichting

---

[31] Zie bijvoorbeeld artikel 8, tweede lid, en de toelichting op dit artikellid. Deze bepaling is, ook met de toelichting erbij, niet zonder meer duidelijk. Zorgverzekeraars en zorgverleners hebben immers het recht het BSN te gebruiken. Daar komt bij dat de bepaling zelf een onbepaalde, en daardoor onbeperkte, mogelijkheid biedt om – bij ministeriële regeling – te bepalen dat publieke identificatiemiddelen kunnen worden gebruikt buiten de publieke sector.

[32] Artikel 14.

[33] Verordening (EU) 2016/679 van het Europees Parlement en de Raad, 27 april 2016, betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG, PB 2016, L 119. De verordening treedt in werking op 25 mei 2018.

[34] Richtlijn nr. 95/46/EG van het Europees Parlement en de Raad van de Europese Unie van 23 november 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (Pb 1995, L 281).

aangesneden onderwerpen.[35] Daarop gaat de toelichting niet in. Voor zover de AVG wel ruimte biedt voor dergelijke regels gaat de Afdeling er van uit dat in dat kader passende aandacht zal worden geschonken aan de vraag hoe burgers begrijpelijk en nauwkeurig worden geïnformeerd over keuzes, toestemmingen en machtigingen die zij worden geacht te maken en te geven.

De Afdeling adviseert in de toelichting op het bovenstaande in te gaan en het wetsvoorstel zo nodig aan te passen.

b. Inloggen door een ander dan de burger

De Afdeling vraagt voorts aandacht voor het fenomeen van inloggen door een ander dan de burger zelf. Bij ministeriële regeling kan worden bepaald dat een publiek inlogmiddel kan worden gebruikt om aangewezen organisaties toegang te geven tot een systeem voor de elektronische uitwisseling van gegevens. Volgens de toelichting kan het gaan om de uitwisseling van patiëntgegevens binnen en tussen zorginstellingen. Gebruik van een publiek identificatiemiddel is van belang om zeker te weten dat het om de juiste persoon gaat, aldus de toelichting.[36]

Het artikel en de toelichting zijn niet duidelijk waar het gaat om de rol van de burger. Indien de bepaling inhoudt dat het identificatiemiddel (en de gegevens die met een identificatiemiddel kunnen worden gegenereerd) niet wordt gebruikt door de burger zelf maar door een zorginstelling, zonder dat de burger daarvan op de hoogte is, dan staat dat haaks op het stelsel. Een identificatiemiddel is immers een middel in handen van de burger, die met dat middel toegang krijgt tot een elektronische systeem van een bestuursorgaan of bijvoorbeeld een zorginstelling. Hij is de unieke gebruiker van dat middel. Om diezelfde reden mogen burgers ook niet toestaan dat een ander een fotokopie maakt van hun paspoort of identiteitskaart. De Afdeling adviseert de bepaling te heroverwegen of nauwkeuriger te formuleren.

4. Bescherming van persoonsgegevens

Inzake de bescherming van persoonsgegevens heeft de Afdeling twee aandachtspunten.

In de eerste plaats adviseert de Afdeling aan te geven in hoeverre er onder het regime van de AVG nog ruimte is om nadere regels te stellen die verband houden met de verwerking van persoonsgegevens. In aansluiting hierop is de memorie van toelichting aangevuld met een passage met de strekking dat nationale regels met betrekking tot onder meer grondslagen, doelen, waarborgen en beveiliging noodzakelijk zijn, juist om een goede uitvoering van de AVG te bewerkstelligen.

Voorts vraagt de Afdeling aandacht voor het gebruik van een publiek middel binnen interne systemen. Anders dan de Afdeling veronderstelt, is in dat geval geen sprake van een burger die zijn middel uit handen geeft, maar van de situatie dat de houder van een publiek middel zijn eigen middel intern gebruikt als zorgverlener. Dit punt zal in de toelichting worden verduidelijkt.

---

[35] Zie de onderwerpen besproken in paragraaf 4 (Privacy) van de toelichting.
[36] Artikel 8, derde lid, en de toelichting op dat artikel.

5. Machtiging en elektronische handtekening

a. Betrouwbaarheidsniveaus bij machtiging

Natuurlijke personen, bedrijven en organisaties kunnen elektronisch gemachtigd worden om in te loggen namens een natuurlijk persoon, bedrijf of organisatie.[37] Het voorstel stelt geen eisen aan de betrouwbaarheid van zulke machtigingen. Dit contrasteert sterk met de regels voor inloggen zelf, die gebaseerd zijn op een uitgewerkt stelsel van betrouwbaarheidsniveaus.

- *Een stelsel van machtigingen zal tenminste aan dezelfde betrouwbaarheidseisen moeten voldoen als het stelsel van identificatiemiddelen: als een bestuursorgaan alleen elektronische identificatie op betrouwbaarheidsniveau substantieel of hoog accepteert, zal ook identificatie via machtiging op dat niveau moeten plaatsvinden.*
- *Daarnaast zal onderzocht moeten worden welke aanvullende eisen zullen moeten gelden ter bescherming van de persoon die de machtiging verleent. Zo kan worden bepaald dat een machtiging alleen betrekking heeft op nauwkeurig omschreven handelingen en dat de machtiging voor een beperkte periode geldt.[38]*

De Afdeling adviseert het voorstel op deze punten aan te passen.

b. Gebruik van DigiD als elektronische handtekening

DigiD wordt in sommige gevallen gebruikt als elektronische handtekening, bij voorbeeld om de elektronische aangifte inkomstenbelasting te ondertekenen. Bovendien wordt DigiD Machtigen in sommige gevallen gebruikt om namens de gemachtigde een elektronische handtekening te zetten. Voor deze toepassingen lijkt onvoldoende wettelijke grondslag te bestaan.[39] Indien het de bedoeling is dat DigiD en andere identificatiemiddelen en middelen voor elektronische machtiging, ook in de toekomst, zullen worden gebruikt als elektronische handtekening, acht de Afdeling het van belang dit wettelijk te regelen.

De Afdeling adviseert het voorstel met dit punt aan te vullen.

5. Machtiging en elektronische handtekening

Inzake machtiging en elektronische handtekening adviseert de Afdeling aanpassing van het voorstel op de volgende punten.

In de eerste plaats stelt de Afdeling dat het voorstel geen eisen stelt aan de betrouwbaarheid van machtigingen; het betrouwbaarheidsniveau van een machtiging zou gekoppeld moeten zijn aan dat van het identificatiemiddel.
In reactie hierop wordt het volgende opgemerkt. Primair van belang is de mate van zekerheid over de identiteit van de machtiginggever op het moment van registratie van de machtiging (betrouwbaarheid bevoegdheidsverklaring). De te registreren gegevens over de gemachtigde moeten dan juist zijn, opdat het bestaan van een betrouwbare relatie aannemelijk is. Hoe complexer het registratieproces, des te betrouwbaarder de machtiging. Het is, met inachtneming van de te op te stellen ministeriële

---

[37] Artikelen 5, eerste lid, onderdeel b, en 11, tiende lid.
[38] Vergelijk artikel 5, tweede en zesde lid, van de Regeling voorzieningen GDI.
[39] DigiD wordt alleen geregeld in de Regeling voorzieningen GDI en daar gedefinieerd als een middel voor de toegang tot elektronische dienstverlening (artikel 1). Daar wordt aan toegevoegd dat DigiD alleen mag worden gebruikt voor het doel waarvoor het is bestemd (artikel 3, zevende lid).

regeling terzake, aan de desbetreffende publieke dienstverlener (bestuursorgaan of aangewezen organisatie) om te bepalen op welk betrouwbaarheidsniveau een gebruiker zich moet identificeren om toegang te krijgen tot een elektronische dienst. Dit geldt eveneens voor de toegang voor gemachtigden. Met andere woorden: de dienstverlener bepaalt in beginsel ook het betrouwbaarheidsniveau van een machtiging. Het lijkt logisch dat dienstverleners de betrouwbaarheidsniveaus altijd zullen koppelen. Dit is echter niet zonder meer het geval. Reden hiervoor is dat hoogbetrouwbare machtiging, en dus een complex registratieproces terzake, afbreuk doet aan het gebruiksgemak voor degene die een elektronische dienst wil afnemen; hij/zij ervaart dan een hoge drempel om te machtigen. Dienstverleners willen dat voorkomen en zullen, afhankelijk van de aard van hun dienstverlening en de gebruikers, de betrouwbaarheidsniveaus niet koppelen door inlogmiddelen van eenzelfde betrouwbaarheidsniveau te vereisen. Dit hoeft niet problematisch te zijn. Op basis van een risicoafweging kan de dienstverlener na het moment van machtiging nog een andere technische of fysieke vorm van controle laten plaatsvinden. Van belang is dat de identiteitsvaststelling bij het registeren van de machtigingsrelatie op een vergelijkbaar betrouwbaarheidsniveau plaatsvindt als het vereiste niveau voor afname van de dienst. Die identiteitsvaststelling dient met voldoende waarborgen te zijn omkleed, gegeven het betrouwbaarheidsniveau waarop de dienstverlening moet plaatsvinden. De op te stellen ministeriële regeling terzake verschaft de kaders daarvoor.

Het wetsvoorstel en de toelichting zijn op dit punt aangepast en verduidelijkt.

Voorts adviseert de Afdeling te onderzoeken welke aanvullende eisen er moeten gelden ter bescherming van de gemachtigde. In reactie hierop zij er op gewezen, dat hierover voorschriften zijn opgenomen in de Regeling voorzieningen gdi, onder meer met betrekking tot reikwijdte en geldigheid van de machtiging bij dienstverlening aan een natuurlijke persoon (burger). Ook op basis van dit wetsvoorstel (artikel 10, tweede lid) zijn hierover regels voorzien. De toelichting is op dit punt verduidelijkt.

Tot slot adviseert de Afdeling het gebruik van elektronische identificatiemiddelen als elektronische handtekening wettelijk te verankeren. In reactie hierop wordt het volgende opgemerkt. Ik onderken het door de Afdeling gestelde dat het huidige DigiD in de praktijk niet alleen als elektronisch identificatiemiddel wordt gebruikt, maar feitelijk ook als elektronische handtekening. Het gaat hierbij om verschillende rechtsfiguren met een eigen functie en rechtsgevolgen (identificatie/authenticatie respectievelijk wilsuiting), zoals ook blijkt uit de eidas-verordening. Voorzover DigiD aan de (veiligheids- en betrouwbaarheids)eisen voor een elektronische handtekening voldoet, is een dergelijk gebruik echter niet bezwaarlijk of verboden, noch is voor dit gebruik een specifieke wettelijke grondslag vereist. Primair van belang is dat een dienstverlener, bijvoorbeeld de Belastingdienst, gebruikers informeert wanneer bij het gebruik van DigiD sprake is van identificatie en wanneer van het plaatsen van een handtekening.
Het bieden van meer duidelijkheid over het gebruik van elektronische identificatiemiddelen als elektronische handtekening valt buiten de werkingssfeer van dit wetsvoorstel. Mogelijk bestaat in de toekomst behoefte aan nadere regulering. Overwogen zal dan worden of opname in latere wijziging (uitbreiding) van de voorgestelde wet opportuun is.

6. Verhouding tussen wet en uitvoeringsregelingen

a. Algemeen

In haar advies over het voorstel van wet modernisering elektronisch bestuurlijk verkeer heeft de Afdeling opgemerkt dat is beoogd het voorstel techniekonafhankelijk vorm te geven, maar dat in dat wetsvoorstel onder de abstracte, moeilijk te begrijpen formuleringen in feite concrete begrippen worden aangeduid. Het gaat dan om begrippen als MijnOverheid, berichtenbox en contact- of webformulieren. De Afdeling adviseerde die begrippen in het voorstel zelf uitdrukkelijk te noemen en de abstracte termen achterwege te laten.[40]

Het nu voorliggende voorstel is eveneens abstract en techniekonafhankelijk geformuleerd. De uitwerking van de abstracte begrippen wordt gedelegeerd aan lagere regelgeving. Zo zijn begrippen als DigiD, MijnOverheid, DigiD Machtigen en het BSN-Koppelregister geregeld in de (ministeriële) Regeling voorzieningen GDI, die – met aanpassingen – onder het wetsvoorstel zal komen te hangen. Het is aannemelijk dat MijnOverheid en het BSN-Koppelregister, die een centrale plaats innemen in de communicatie tussen overheid en burger, de komende jaren zullen blijven bestaan. Het is meer passend om deze centrale onderdelen van de generieke digitale infrastructuur in de wet zelf te regelen.

De Afdeling adviseert de hoofdzaken van de Regeling voorzieningen GDI in de wet zelf op te nemen.

b. Uitgifte van identificatiemiddelen

De Minister van BZK is verantwoordelijk voor de uitgifte van DigiD op niveau laag, en op termijn voor de uitgifte van DigiD op hogere niveaus. Het voorstel geeft hem wel de verantwoordelijkheid voor de generieke digitale infrastructuur, maar niet voor de uitgifte van deze publieke identificatiemiddelen. In lijn met punt 1 van dit advies, waarin wordt benadrukt dat de Minister voldoende bevoegdheden moet hebben om zijn verantwoordelijkheid voor het stelsel waar te maken, adviseert de Afdeling de verantwoordelijkheid voor dit centrale onderdeel van het stelsel wettelijk te regelen.

6. Verhouding tussen wet en uitvoeringsregelingen

Inzake de verhouding tussen wet en uitvoeringsregelingen gaat de Afdeling in op twee punten.

In de eerste plaats adviseert de Afdeling om in het wetsvoorstel, dat techniekonafhankelijk is geformuleerd, de centrale onderdelen van de gdi op te nemen. In reactie hierop zij opgemerkt dat ik met de Afdeling van mening ben dat te abstracte formulering afbreuk doet aan de duidelijkheid en rechtszekerheid. Om die reden bevat het wetsvoorstel de functionaliteiten van een aantal belangrijke voorzieningen (centrale onderdelen), waarbij concretisering, waaronder de begrippen, en uitwerking in algemene maatregelen van bestuur en ministeriële regelingen plaatsvindt. De grondslagen hiervoor worden in het wetsvoorstel ingekaderd en begrensd. Middels deze systematiek wordt een zekere mate van toekomstbestendigheid en flexibiliteit bewerkstelligd.

---

[40] Advies no. W04.17.0190 van 15 maart 2018, punt 4.

Voorts adviseert de Afdeling de verantwoordelijkheid van de Minister van BZK voor de uitgifte van publieke identificatiemiddelen wettelijk te regelen. In dit verband zij er op gewezen dat artikel 5 eerste lid, onder a, van het wetsvoorstel de zorgplicht voor de Minister van BZK bevat voor infrastructuur voor de uitgifte aan en het gebruik van publieke identificatiemiddelen op verschillende betrouwbaarheidsniveaus. Deze verantwoordelijkheid wordt uitgewerkt in lagere regelgeving.

7. Redactionele kanttekeningen

De Afdeling verwijst naar de bij dit advies behorende redactionele bijlage.

7. Redactionele kanttekeningen

Aan de redactionele opmerkingen is voor een deel gevolg gegeven.

8.

Bij gelegenheid van dit nader rapport zijn tevens enkele wijzigingen, zowel van inhoudelijke als technische aard, in het wetsvoorstel aangebracht. Deze hebben primair betrekking op de artikelen aangaande de bedrijfs- en organisatiemiddelen. Bij de voorbereiding van de nadere uitwerking bij algemene maatregel van bestuur is namelijk gebleken dat een aantal aanpassingen wenselijk is om het stelsel goed te laten functioneren. Zo is het wetsvoorstel aangevuld met kaders voor het intrekken van een erkenning op verzoek van de erkende partij en is een grondslag opgenomen om bij de erkenning gebruik te kunnen maken van een certificerende instantie. Tevens is, mede naar aanleiding van de redactionele opmerking van de Afdeling inzake registers met attributen, besloten de erkenning van attributendiensten te vervangen door een bevoegdheid van de Minister om attributen aan te wijzen. Dit past beter bij de omstandigheid dat de attributen die van belang kunnen zijn voor de betrouwbare toegang van ondernemingen en rechtspersonen, voornamelijk gevat zijn in publiekrechtelijke registers, zoals een beroepsregister. Voorts is artikel 7 van het wetsvoorstel aangevuld met een bepaling inzake de acceptatie van een erkend bedrijfs- en organisatiemiddel ingeval dienstverlening aan een natuurlijke persoon (burger) plaatsvindt door tussenkomst (machtiging) van een bedrijf. Tot slot is het overgangsrecht inzake het gebruik van een middel met een lager betrouwbaarheidsniveau verplaatst naar artikel 6.

De Afdeling advisering van de Raad van State geeft U in overweging het voorstel van wet niet te zenden aan de Tweede Kamer der Staten-Generaal dan nadat met het vorenstaande rekening zal zijn gehouden.

De vice-president van de Raad van State,
J.P.H. Donner

Ik moge U hierbij verzoeken het hierbij gevoegde gewijzigde voorstel van wet en de gewijzigde memorie van toelichting aan de Tweede Kamer der Staten-Generaal te zenden.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
R.W. Knops

Redactionele bijlage bij het advies van de Afdeling advisering van de Raad van State betreffende no.W04.17.0400/I

- In het wetsvoorstel zelf tot uitdrukking brengen dat het voorstel een eerste tranche van regelgeving voor digitalisering van de overheid bevat (de citeertitel wekt een verwachting die nu nog niet wordt waargemaakt). In de toelichting uitvoeriger ingaan op de volgende tranches dan nu gebeurt (paragraaf I.1 (Aanleiding)).
- In artikel 1 het begrip «elektronische dienstverlening» vervangen door een neutralere term (bijvoorbeeld elektronische communicatie of elektronisch berichtenverkeer), om te voorkomen dat handelingen zoals het intrekken van een vergunning, het opleggen van een last onder bestuursdwang en het opleggen van een bestuurlijke boete worden gekwalificeerd als dienstverlening.
- In artikel 1 een definitie opnemen van «de voorziening, bedoeld in artikel 5, eerste lid, onderdeel b,», bijvoorbeeld: elektronische machtiging. Die term kan dan gebruikt worden in de artikelen 8, eerste, tweede en derde lid, en 10, tweede lid.
- Eén begrip introduceren en definiëren dat zowel bestuursorganen als aangewezen organisaties omvat; de term «bestuursorgaan» niet gebruiken in een betekenis die afwijkt van die in de Algemene wet bestuursrecht (artikel 2, eerste lid).
- Punt 3 van het advies van de Afdeling advisering van 12 februari 2018 over het Tijdelijk besluit digitale toegankelijkheid overheid, zaak W04.18.0021, in acht nemen bij het aanwijzen van standaarden op basis van artikel 3. Voorts de afbakening van organisaties in artikel 3 afstemmen op artikel 1 van dat Tijdelijk besluit.
- Artikel 3 onderbrengen in een afzonderlijk hoofdstuk: het artikel regelt een apart onderwerp en betreft een grotere groep organisaties dan de rest van het voorstel.
- Artikel 4 overbrengen naar en combineren met artikel 6. In het tweede lid regelen aan welke eisen een auditor moet voldoen (de in de wetgeving meeste gebruikelijke betekenis – controleur van jaarrekeningen – zal hier niet zijn bedoeld).
- De regels voor authenticatiediensten, attributendiensten, machtigingsdiensten en ontsluitende diensten niet opnemen in § 4.3 (Elektronische dienstverlening aan bedrijven), nu die diensten (blijkens de definities in artikel 1) ook gaan over identificatie van of namens natuurlijke personen.
- Artikel 11, negende lid, uitbreiden tot registers waarin natuurlijke personen zijn opgenomen, nu het blijkens de toelichting op het artikel mede gaat om het BIG-register.
- In artikel 25 verduidelijken dat bij een experiment alleen kan worden afgeweken van het verbod om andere dan toegelaten middelen te accepteren, nu dat blijkens de toelichting de bedoeling is. Voorts aanwijzing 2.42, tweede lid, met toelichting, van de Aanwijzingen voor de regelgeving (Ar) in acht nemen.
- Artikel 26 achterwege laten, nu dit al is geregeld (artikel XI, derde lid, van de Wet elektronisch berichtenverkeer belastingdienst).
- Te zijner tijd de verwijzing naar artikel X van de Wet elektronisch berichtenverkeer belastingdienst in artikel 2:17, tweede lid, van het voorstel van wet modernisering elektronisch bestuurlijk verkeer vervangen door een verwijzing naar artikel 5 van de Wet digitale overheid.
- De Regeling voorzieningen GDI omhangen. Voorts een bepaling opnemen waarin de zelfstandige algemene maatregel van bestuur ter implementatie van EU-richtlijn 2016/2102 wordt omgehangen naar artikel 3, tweede en derde lid.
- Artikel 29, derde lid, zo aanpassen dat het tijdstip waarop de acceptatieplicht (artikelen 7 en 13) ingaat voor de verschillende bestuursorga-

nen en aangewezen organisaties blijkt uit een Staatsblad of de Staatscourant (kenbaarheidsvereiste, vergelijk aanwijzing 4.15 Ar), bijvoorbeeld door te bepalen dat het aansluitschema wordt gepubliceerd in de Staatscourant.