STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 37158
29 oktober 2015

Regeling van de Minister van Binnenlandse Zaken en Koninkrijksrelaties van 23 oktober 2015, nr. 2015-609536, houdende regels met betrekking tot de werking, beveiliging en betrouwbaarheid van de voorzieningen voor elektronisch berichtenverkeer en informatieverschaffing alsmede van voorzieningen voor elektronische authenticatie en elektronische registratie van machtigingen (Regeling voorzieningen GDI)

De Minister van Binnenlandse zaken en Koninkrijksrelaties

Gelet op artikel X, tweede lid, van de Wet elektronisch berichtenverkeer Belastingdienst;

Besluit:

HOOFDSTUK 1 ALGEMENE BEPALINGEN

Artikel 1 Definities

In deze regeling wordt verstaan onder:
MijnOverheid: de voorziening die bereikbaar is via het webadres mijn.overheid.nl voor de dienst voor elektronisch berichtenverkeer de Berichtenbox, en de diensten voor informatieverschaffing Lopende Zaken en Persoonlijke gegevens;
DigiD-voorziening: de voorziening voor elektronische authenticatie en voor uitgifte van elektronische authenticatiemiddelen die bereikbaar is via het webadres www.digid.nl;
DigiD: een via de DigiD-voorziening aan gebruiker verstrekt middel voor de toegang tot elektronische dienstverlening;
DigiD Machtigen: de voorziening voor elektronische registratie van machtigingen die bereikbaar is via het webadres machtigen.digid.nl;
BSN-Koppelregister: een voorziening die een relatie legt tussen een uniek identificerend kenmerk op een privaat authenticatiemiddel en het burgerservicenummer van de houder;
vertegenwoordigde: een natuurlijk persoon die zich ter behartiging van zijn belangen in het verkeer met afnemers van DigiD Machtigen laat vertegenwoordigen door een gemachtigde;
gemachtigde: een gebruiker van DigiD Machtigen die bevoegd is namens de vertegenwoordigde bepaalde (rechts)handelingen te verrichten;
overheidsorgaan:
1° een orgaan van een rechtspersoon die krachtens publiekrecht is ingesteld, of
2° een ander persoon of college, met enig openbaar gezag bekleed;
afnemer: een overheidsorgaan dat, of een rechtspersoon met een wettelijke taak, niet zijnde een overheidsorgaan, die bij de uitoefening van zijn taak of bevoegdheid gebruik maakt van MijnOverheid of een dienst aanbiedt voor elektronisch verkeer en daarbij gebruik maakt van DigiD respectievelijk DigiD Machtigen;
private authenticatiedienst: een private leverancier van authenticatiemiddelen;
privaat authenticatiemiddel: een voorziening voor elektronische authenticatie, geleverd door een private authenticatiedienst, waarmee toegang kan worden verkregen tot elektronische diensten;
gebruiker van een privaat authenticatiemiddel: een natuurlijk persoon die bij een private authenticatiedienst een authenticatiemiddel aanschaft;
beveiligingsincident: een gebeurtenis die een bedreiging vormt voor de betrouwbaarheid, integriteit, vertrouwelijkheid of de beschikbaarheid van de voorzieningen waarop deze regeling betrekking heeft;
Minister: de Minister van Binnenlandse Zaken en Koninkrijksrelaties.

HOOFDSTUK 2 VOORZIENINGEN VOOR ELEKTRONISCH BERICHTENVERKEER EN INFORMATIEVERSCHAFFING

Artikel 2 Gebruik MijnOverheid

1. De Minister maakt een MijnOverheid-account aan voor een ieder die:
   a. de leeftijd van 14 jaar heeft bereikt;
   b. beschikt over een burgerservicenummer;
   c. woonachtig is in Nederland of de Nederlandse nationaliteit heeft; en
   d. beschikt of kan beschikken over een DigiD.

2. De gebruiker neemt door het activeren van zijn MijnOverheid-account dit account in gebruik. Hij maakt tevens kenbaar dat hij langs elektronische weg bereikbaar is voor het ontvangen van berichten in de Berichtenbox van door hem geselecteerde afnemers.

3. De gebruiker heeft toegang tot zijn MijnOverheid-account door gebruikmaking van DigiD.

4. De gebruiker kan de selectie van afnemers, waarvan hij berichten in zijn Berichtenbox wil ontvangen, wijzigen.

5. Het tweede lid, tweede zin, en het vierde lid zijn niet van toepassing met betrekking tot afnemers voor wie het gebruik van MijnOverheid wettelijk is voorgeschreven.

6. Het MijnOverheid-account is strikt persoonlijk en niet overdraagbaar.

7. Het MijnOverheid-account mag alleen gebruikt worden voor het doel waarvoor het is bestemd.

8. De Minister kan het MijnOverheid-account opheffen na het overlijden van de gebruiker of ingeval de gebruiker niet langer voldoet aan een of meer van de in het eerste lid genoemde criteria.

HOOFDSTUK 3 VOORZIENINGEN VOOR ELEKTRONISCHE AUTHENTICATIE

Artikel 3 Gebruik DigiD

1. DigiD kan alleen door de beoogde gebruiker worden aangevraagd. Een aanvraag geschiedt via www.digid.nl of, indien het tweede lid onder c, van toepassing is, via www.svb.nl.

2. DigiD wordt slechts verstrekt aan een beoogde gebruiker die:
   a. als ingezetene is ingeschreven in de basisregistratie personen en uit dien hoofde een burgerservicenummer heeft;
   b. als niet-ingezetene is ingeschreven in de basisregistratie personen, een burgerservicenummer heeft en bovendien de Nederlandse nationaliteit heeft; of
   c. als niet-ingezetene is ingeschreven in de basisregistratie personen, een burgerservicenummer heeft, een AOW-pensioen ontvangt en klant is van de Sociale Verzekeringsbank.

3. De Minister verstrekt DigiD na verificatie van de verstrekte gegevens door de aanvrager.

4. De gebruiker kan met de verstrekte DigiD toegang verkrijgen tot een dienst van een afnemer zodra hij DigiD heeft geactiveerd.

5. DigiD is strikt persoonlijk en niet overdraagbaar.

6. DigiD wordt alleen gebruikt voor het doel waarvoor het is bestemd.

7. DigiD vervalt drie jaar nadat deze voor het laatst is gebruikt.

8. De gebruiker kan de Minister verzoeken om zijn DigiD te laten blokkeren of op te heffen.

Artikel 4 BSN-Koppelregister

1. De gebruiker van een privaat authenticatiemiddel, die dit middel wil gebruiken voor de afname van diensten in het publieke domein, maakt dit kenbaar aan de private authenticatiedienst van zijn keuze.

2. De private authenticatiedienst die de mogelijkheid, bedoeld in het eerste lid, biedt, schakelt het BSN-Koppelregister in, teneinde het voor gebruiker mogelijk te maken met zijn authenticatiemiddel toegang te verkrijgen tot elektronische diensten in het publieke domein.

HOOFDSTUK 4 VOORZIENINGEN VOOR ELEKTRONISCHE REGISTRATIE VAN MACHTIGINGEN

Artikel 5 Gebruik DigiD Machtigen

1. Een vertegenwoordigde of beoogd gemachtigde kan een aanvraag tot registratie van een machtiging doen via machtigen.digid.nl of via een afnemer die het aanvragen faciliteert.

2. De aanvraag en registratie van een machtiging kunnen betrekking hebben op een of meerdere

diensten van een of meerdere afnemers en kennen een vooraf bepaalde geldigheidsduur.

3. De Minister keurt de aanvraag goed na verificatie van de verstrekte gegevens door de vertegenwoordigde en beoogd gemachtigde of derde.

4. De vertegenwoordigde geeft de ontvangen machtigingscode en zijn burgerservicenummer aan de gemachtigde.

5. De gemachtigde accepteert de machtiging door de registratie van de machtiging te activeren via machtigen.digid.nl of via een afnemer die dat faciliteert. Hij voert hiertoe de machtigingscode en het burgerservicenummer van vertegenwoordigde in.

6. De registratie van een machtiging eindigt door het intrekken van de geregistreerde machtiging of na het verstrijken van de geldigheidsduur.

7. De registratie van de machtiging kan worden ingetrokken via machtigen.digid.nl of via een afnemer die dat faciliteert.

8. De vertegenwoordigde en de gemachtigde kunnen een overzicht van aangevraagde en geactiveerde registraties van machtigingen opvragen. Het overzicht kan worden ingezien via machtigen-.digid.nl.

HOOFDSTUK 5 WERKING, BEVEILIGING EN BETROUWBAARHEID

Artikel 6 Veiligheid

1. Teneinde de veiligheid, betrouwbaarheid, beschikbaarheid en continuïteit van MijnOverheid, DigiD, DigiD Machtigen en het BSN-Koppelregister te waarborgen, neemt de Minister passende maatregelen om inbreuken op en aantastingen van de beveiliging en de processen van de voorzieningen te voorkomen. Hierbij wordt in ieder geval voldaan aan:
   a. de open normen en standaarden op de 'pas-toe-of-leg-uit-lijst' van het Forum Standaardisatie;
   b. de normen ICT-beveiligingsassessments DigiD;
   c. de Baseline Informatiebeveiliging Rijksdienst; en
   d. de Voorschriften Informatiebeveiliging Rijksdienst.

2. Het BSN-Koppelregister voldoet tevens aan de veiligheidseisen uit het afsprakenstelsel elektronische toegangsdiensten bedoeld in artikel 1 van het Instellingsbesluit besturing elektronische toegangsdiensten.

3. De in het eerste en tweede lid bedoelde maatregelen worden getroffen en onderhouden op basis van daartoe na een risicoanalyse vastgestelde informatiebeveiligingsplannen.

4. Teneinde maatregelen te kunnen aanpassen en doorontwikkeling mogelijk te maken, wordt voor de voorzieningen of onderdelen daarvan onderhoud gepleegd. Hiertoe kunnen, na voorafgaande bekendmaking, de voorzieningen of onderdelen daarvan tijdelijk buiten gebruik worden gesteld.

Artikel 7 Maatregelen

1. De Minister kan zonder voorafgaande bekendmaking de toegang tot of de beschikbaarheid van MijnOverheid, DigiD, DigiD Machtigen en het BSN-Koppelregister onderbreken, indien sprake is van een storing of aantasting van de betrouwbaarheid van de voorziening of van een beveiligingsincident. Indien mogelijk wordt voorafgaand informatie verstrekt over de aard en verwachte duur van de onderbreking. Dit geschiedt voor MijnOverheid, DigiD en DigiD Machtigen via mijn.overheid.nl, www.digid.nl of machtigen.digid.nl.

2. Teneinde aantasting van de beveiliging of misbruik of oneigenlijk gebruik van MijnOverheid, DigiD, DigiD Machtigen en het BSN-Koppelregister te signaleren en adequaat te beëindigen, kan de Minister:
   a. controles uitvoeren op de gegevens die beschikbaar zijn binnen de in deze regeling bedoelde voorzieningen;
   b. bij het vermoeden van misbruik of oneigenlijk gebruik de toegang tot de voorziening onderbreken; of
   c. bij geconstateerd misbruik of oneigenlijk gebruik de toegang tot de voorziening beëindigen.

HOOFDSTUK 6 SLOTBEPALINGEN

Artikel 8 Intrekking besluiten

De volgende besluiten worden ingetrokken:
a. het Besluit beheer Persoonlijke Internetpagina;
b. het Besluit beheer DigiD;
c. het Besluit vaststelling aansluitvoorwaarden MijnOverheid.nl.

Artikel 9 Inwerkingtreding

Deze regeling treedt in werking met ingang van 1 november 2015.

Artikel 10 Citeertitel

Deze regeling wordt aangehaald als: Regeling voorzieningen GDI.

Deze regeling zal met de toelichting in de Staatscourant worden geplaatst.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
R.H.A. Plasterk

TOELICHTING

1. Inleiding; doel van de regeling

Op grond van de Wet elektronisch berichtenverkeer Belastingdienst (hierna: de wet) vindt in beginsel alle berichtenverkeer tussen de belastingplichtige en de Belastingdienst uitsluitend nog elektronisch plaats. In de formele wetten voor de belastingen, toeslagen en de invordering zijn in de wet bepalingen opgenomen die het juridische kader scheppen voor het verder ontwikkelen van elektronisch berichtenverkeer. Om dit mogelijk te maken en het fiscale deel van de wet uitvoerbaar te laten zijn, is in artikel X, een wettelijke basis gerealiseerd voor de voorzieningen inzake de generieke digitale infrastructuur (GDI).
Het eerste lid van artikel X bepaalt dat Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties zorg draagt voor de inrichting, beschikbaarstelling, instandhouding, werking, beveiliging en betrouwbaarheid van voorzieningen voor elektronisch berichtenverkeer en informatieverschaffing alsmede van voorzieningen voor elektronische authenticatie en elektronische registratie van machtigingen.
De GDI, die het mogelijk maakt dat overheidsinstanties digitaal gaan functioneren, is in de wet functioneel omschreven, teneinde nieuwe of geactualiseerde voorzieningen en (technische) ontwikkelingen te kunnen opvangen. In dit verband functioneren momenteel de voorzieningen MijnOverheid (met als primaire – onder meer door de Belastingdienst gebruikte – onderdeel de Berichtenbox), DigiD, DigiD Machtigen en het BSN-koppelregister.
Het derde lid van artikel X van de wet bepaalt dat Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties persoonsgegevens verwerkt, waaronder het burgerservicenummer, voor zover dit noodzakelijk is voor de goede vervulling van de taak, bedoeld in het eerste lid; bij algemene maatregel van bestuur wordt nader bepaald welke persoonsgegevens worden verwerkt, aan wie deze worden verstrekt en hoe lang deze worden bewaard. Hieraan zal uitvoering worden gegeven met het Besluit verwerking persoonsgegevens GDI.
Het tweede lid van artikel X van de wet bepaalt dat bij regeling van Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties regels worden gesteld met betrekking tot de werking, beveiliging en betrouwbaarheid van de voorzieningen, bedoeld in het eerste lid. Ter uitvoering hiervan wordt met de onderhavige regeling beoogd duidelijkheid en rechtszekerheid te bieden aan gebruikers en afnemers (publieke dienstverleners) door te omschrijven welke eisen worden gesteld aan de werking, beveiliging en betrouwbaarheid van de betrokken GDI-voorzieningen teneinde inbreuken op de (technische) beveiliging en het proces zoveel mogelijk te voorkomen en te herstellen. Het betreft deels bepalingen van technische en administratieve aard, die bovendien regelmatig aan wijziging en actualisering onderhevig zijn. Voorts is sprake van bestaande, in de praktijk gehanteerde voorschriften en processen, die met deze regeling van een deugdelijke grondslag worden voorzien.
Het kabinet werkt toe naar het digitaal communiceren door en met de overheid en betere publieke dienstverlening. Dit is opgenomen in het Regeerakkoord 2012 en uitgewerkt in de Visiebrief Digitaal 2017 (TK 26 643, nr. 280). Deze regeling maakt derhalve onderdeel uit van een groter geheel; naast het wettelijk verankeren van de generieke digitale infrastructuur, maakt bijvoorbeeld ook de invoering van het eID-stelsel (private authenticatie op een hoog betrouwbaarheidsniveau, ontwikkeld door overheid en bedrijfsleven gezamenlijk; thans Idensys genaamd) en het doorontwikkelen van publieke authenticatie (thans: DigiD) hiervan deel uit. Genoemde ontwikkelingen komen samen in de wet- en regelgeving rond de elektronische overheid.

2. Reikwijdte van de regeling

In de praktijk functioneren de volgende GDI-voorzieningen in relatie tot burgers:
MijnOverheid: een gepersonaliseerde elektronische voorziening waarmee voor burgers een persoonlijk domein beschikbaar komt dat geschikt is voor informatieverschaffing door de overheid. Deze voorziening bestaat – thans – uit de dienst voor elektronisch berichtenverkeer de Berichtenbox, en de diensten voor informatieverschaffing Lopende Zaken en Persoonlijke gegevens.
DigiD: de publieke voorziening voor elektronische authenticatie in het verkeer met de overheid cq instanties in het publieke domein. Deze voorziening voorziet ook in de uitgifte van elektronische authenticatiemiddelen voor de toegang tot elektronische dienstverlening. In het maatschappelijk verkeer wordt de term 'DigiD' gehanteerd om zowel de voorziening als het (publieke) middel aan te duiden. In deze regeling wordt omwille van de duidelijkheid onderscheiden tussen 'DigiD-voorziening' en 'DigiD', waarbij de term 'DigiD' ter aanduiding van het middel wordt gehanteerd. Met DigiD kan toegang worden verkregen tot onder meer MijnOverheid, op dit moment op twee betrouwbaarheidsniveaus: via identificatie met gebruikersnaam en wachtwoord en via identificatie met gebruikersnaam, wachtwoord en sms-code. Op dit moment wordt het gebruik van een DigiD-app als vervanging van sms onderzocht. Ook heeft het kabinet het voornemen aan DigiD een voorziening toe te voegen op een nog hoger betrouwbaarheidsniveau en oriënteert het zich op de mogelijkheid om DigiD te combineren met een controle langs digitale weg op gegevens van bestaande wettelijke identiteitsdo-

cumenten. In dat kader vinden in 2016 enkele kleinschalige pilots plaats, waarbij voor een beperkt aantal Nederlandse identiteitskaarten een extra functionaliteit wordt toegevoegd aan de bestaande chip met elektronica op deze documenten. Die functionaliteit maakt het mogelijk dat de houder zich in het elektronische verkeer met de overheid op een hoger betrouwbaarheidsniveau kan identificeren dan nu met DigiD mogelijk is. Daarnaast wordt een pilot gehouden met het rijbewijs, waarbij geen extra functionaliteit wordt toegevoegd maar gebruik wordt gemaakt van de chip zoals die daarin reeds is verwerkt. In deze pilots wordt gebruik gemaakt van dezelfde infrastructuur die het gebruik van het bestaande DigiD ondersteunt. Dit betekent dat deze regeling ook van toepassing is op deze nieuwe authenticatiemiddelen voorzover zij in de pilots worden gebruikt.
BSN-koppelregister: een voorziening waardoor het gebruik van private authenticatiemiddelen mogelijk wordt voor het afnemen van elektronische diensten in het publieke domein. Het betreft een nieuwe voorziening, die is ontwikkeld in het kader van de introductie van het eID-stelsel, thans Idensys genaamd, en die het voor afnemers van MijnOverheid (bijvoorbeeld de Belastingdienst, UWV, SVB, gemeenten) mogelijk maakt om naast publieke middelen voor elektronische authenticatie (DigiD) ook private authenticatiemiddelen te accepteren.
DigiD Machtigen: de voorziening voor elektronische registratie van machtigingen; met behulp hiervan kan verkeer tussen de gemachtigde en de overheid worden afgewikkeld met betrekking tot zaken die de vertegenwoordigde betreffen.
Bovenstaande voorzieningen functioneren onder de verantwoordelijkheid van de Minister van Binnenlandse Zaken en Koninkrijksrelaties en worden beheerd door Logius, de dienst digitale overheid.

3. Gevolgen van de regeling

Deze regeling bevat bepalingen met betrekking tot werking, beveiliging en betrouwbaarheid van de genoemde GDI-voorzieningen. Het gaat daarbij primair om bestaande, in de praktijk reeds gehanteerde voorschriften, die thans een wettelijke basis krijgen. Hierdoor zijn de gevolgen van deze regeling beperkt. Adressaten van de regeling zijn burgers (voor wat betreft de bepalingen inzake gebruik van de voorzieningen) en de (Rijks)overheid zelf (voor wat betreft de bepalingen inzake werking en (informatie) veiligheid).
Met betrekking tot MijnOverheid, DigiD en DigiD Machtigen gold tot voor kort dat burgers, die deze voorzieningen wilden gebruiken, expliciet moesten instemmen met de betreffende gebruiksvoorwaarden; het gebruik van de voorzieningen vond immers plaats op basis van vrijwilligheid. Dit is niet langer het geval wanneer sprake is van verplicht gebruik van deze voorzieningen, zoals in het kader van verplichte digitale belastingaangifte, waarin de bovenliggende wet voorziet. In dat geval zijn algemeen verbindende voorschriften noodzakelijk. Vanwege de eveneens in de wet opgenomen basis voor de GDI, is voor wat betreft de gebruiksvoorwaarden gekozen voor een uniform regime, aangezien dat duidelijkheid en rechtszekerheid biedt. Bij gelegenheid van het opstellen van deze regeling zijn de gebruiksvoorwaarden gestroomlijnd en geactualiseerd. Met betrekking tot het BSN-Koppelregister is van belang, dat bij deze voorziening geen directe relatie met gebruikers bestaat. Het is de private authenticatiedienst, waarbij burgers een authenticatiemiddel aanvragen, die het BSN-Koppelregister inschakelt, namelijk wanneer de betreffende burger dit middel tevens wil gebruiken voor de afname van diensten in het publieke domein, bijvoorbeeld het aanvragen van een vergunning of een toeslag.
De gevolgen van deze regeling kunnen als volgt worden geschetst.
Voor wat betreft MijnOverheid, DigiD en DigiD Machtigen geldt, dat gebruikers niet langer toestemming hoeven te geven bij het gebruik van deze voorzieningen en zij dus minder handelingen gaan verrichten. Overigens is, nu de gebruiksvoorwaarden als zodanig zijn vervallen, ten behoeve van de duidelijkheid en kenbaarheid op mijn.overheid.nl en www.digid.nl een verwijzing naar de onderhavige regeling opgenomen. Mogelijk zullen de voorzieningen als aantrekkelijker (want: gebruiksvriendelijker en met een duidelijker status als publieke voorziening) worden beschouwd en zullen ze nieuwe afnemers aantrekken.
Voor wat betreft het BSN-Koppelregister geldt dat burgers van deze voorziening als zodanig niets zullen merken. Wel kunnen zij als voordeel ervaren dat zij, naast DigiD, nu ook met private authenticatiemiddelen in het publieke domein kunnen inloggen en publieke diensten kunnen afnemen. Voor private authenticatiediensten geldt dat zij meer handelingen gaan verrichten, te weten het aanleveren van persoonsgegevens aan het BSN-Koppelregister (zie voor een overzicht van de gegevens die door de Minister worden verwerkt in de voorzieningen voor de generieke digitale infrastructuur DigiD, DigiD Machtigen, MijnOverheid en BSN-Koppelregister: het Besluit verwerking persoonsgegevens GDI). Dit maakt echter deel uit van hun *business case*, met andere woorden: het weegt op tegen de te verwachten commerciële baten. Bovendien legt de onderhavige regeling aan private authenticatiediensten geen verplichting op om private authenticatiemiddelen voor het publieke domein te leveren; private authenticatiediensten mogen zich blijven toeleggen op het authenticatiemiddelen voor het private domein. Maar als ze het publieke domein willen bedienen, kan dit op veilige en betrouwbare wijze via het BSN-Koppelregister geschieden. Dit vormt de kern van de introductie van Idensys.

Op het toepasselijke regime inzake de beveiliging van de voorzieningen wordt hieronder nader ingegaan.

4. Informatiebeveiliging

Informatieveiligheid van de onderhavige GDI-voorzieningen was in de voormalige gebruiksvoorwaarden ruim geformuleerd. De overheid committeerde zich ten opzichte van de gebruikers om adequate beveiligingsmaatregelen te treffen om inbreuken op en aantasting van de (technische) beveiliging en processen van de voorzieningen te voorkomen en te herstellen. In de praktijk werd en wordt dit ingevuld door middel van het uitvoeren van een risicoanalyse en vervolgens toepassen van de relevante overheidsbrede informatiebeveiligingsnormen, die zijn neergelegd in een aantal documenten over beveiliging van ICT-voorzieningen van de overheid.
Voor wat betreft de voorzieningen in deze regeling gaat het primair om de norm NEN-ISO/IEC 27002, de standaarden DNSSEC, TLS, SAML, SPF en DKIM, de Baseline Informatiebeveiliging Rijksdienst (BIR) en de voorschriften informatiebeveiliging Rijksdienst (VIR en VIRBI). Met betrekking tot DigiD en DigiD Machtigen gelden daarnaast de normen inzake ICT-beveiligingsassessments DigiD. Voor het BSN-Koppelregister gelden daarnaast de eisen uit het afsprakenstelsel elektronische toegangsdiensten, die overigens voor een groot deel de hierboven genoemde normen en voorschriften omvatten. Nu de betreffende GDI-voorzieningen een wettelijke basis krijgen, ligt het in de rede ook de in dat verband relevante beveiligingsnormen te verankeren. Dit geschiedt door naar deze normen te verwijzen. Artikel 6, eerste lid, bevat hiertoe een dynamische verwijzing, dat wil zeggen dat deze tevens nadien in werking getreden wijzigingen omvat. Aanpassingen van de desbetreffende (technische) normen werken dus automatisch door en behoeven toepassing. Op deze wijze wordt ingespeeld op toekomstige actualisering vanwege doorontwikkelende inzichten en wordt aangesloten bij hetgeen de overheid zichzelf heeft opgelegd. Immers: de overheid is reeds gehouden tot naleving van deze normen, (open) standaarden en specificaties, welke vervat zijn in beleidsregels, interne (overheids) besluiten en andere instrumenten van (zelf)regulering. Ingevolge het tweede lid van artikel 6 worden de – door de Minister/dienst Logius – te nemen veiligheidsmaatregelen getroffen en onderhouden op basis van daartoe na een risicoanalyse vastgestelde informatiebeveiligingsplannen. Met name zijn hierbij van belang (indicatief):

NEN-ISO/IEC 27002

Deze – Nederlandse en internationale – normalisatienorm inzake informatietechnologie, beveiligingstechnieken en managementsystemen voor informatiebeveiliging is als open standaard vastgesteld door het Forum Standaardisatie (zie: www.forumstandaardisatie.nl). Hoewel normalisatienormen in beginsel van niet-publiekrechtelijke aard zijn – ze behelzen afspraken tussen marktpartijen, gecoördineerd door het Nederlands Normalisatie Instituut, NNI – is met de overheidsbrede adoptatie en implementatie ervan feitelijk sprake van een publiekrechtelijk karakter. Het feit, dat de normen alleen tegen betaling bij het NNI verkrijgbaar zijn en niet gepubliceerd zijn volgens de Bekendmakingswet, staat niet in de weg aan het (mogen) verwijzen naar deze normen in regelgeving (Hoge Raad 22-6-2012, NJB 2012/1527).

Standaarden DNSSEC, TLS, SAML, SPF en DKIM

Deze beveiligingsstandaarden zijn opgenomen op de lijst met toe te passen open standaarden voor de gehele publieke sector (‘pas-toe-of-leg-uit-lijst’) en zijn te raadplegen via www.forumstandaardisatie.nl

Baseline Informatiebeveiliging Rijksdienst (BIR)

Voor de beveiliging van de informatiehuishouding van de rijksdienst geldt het normenkader van de Baseline Informatiebeveiliging Rijksdienst (BIR): een set rijksbrede beveiligingsnormen, teneinde informatie-uitwisseling binnen de overheid te vereenvoudigen. Dit maakt het mogelijk om veilig samen te werken en onderling gegevens uit te wisselen. Ingevolge de BIR weet een overheidsorganisatie dat de gegevens, die verstuurd worden naar een andere overheidsorganisatie, op het juiste beveiligingsniveau worden behandeld. De BIR omvat en specificeert tevens de standaard NEN-ISO/IEC 27002, Vindplaats: www.earonline.nl/index.php/Overzicht_Baseline_Informatiebeveiliging_Rijksdienst_(BIR_2012).

Voorschriften informatiebeveiliging Rijksdienst (VIR en VIRBI)

Het Besluit Voorschrift Informatiebeveiliging Rijksdienst en het Besluit Voorschrift Informatiebeveiliging Rijksdienst – bijzondere informatie voorzien in de verantwoordelijkheidsverdeling met betrekking tot de beveiliging van informatiesystemen. Vindplaats: Strct. 2007, 122 resp. Stcrt. 2013, 15497.

Normen ICT-beveiligingsassessments DigiD

Alle organisaties die DigiD gebruiken (afnemers) moeten voldoen aan de beveiligingsnorm DigiD, gebaseerd op de ICT-richtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum en dit via een ICT-assessment laten toetsen. Vindplaats: www.logius.nl.

Afsprakenstelsel elektronische toegangsdiensten

Voor het BSN-Koppelregister – en dus niet voor de overige GDI-voorzieningen – zijn, naast de bovengenoemde normen en voorschriften, de afspraken van het afsprakenstelsel elektronische toegangsdiensten relevant. Deze, publiek-privaat afgesproken, eisen zijn gericht op het borgen van veiligheid, betrouwbaarheid en continuïteit van het BSN-Koppelregister en van het afsprakenstelsel zelf. De te nemen maatregelen zijn vervat in normen, (open) standaarden en specificaties en hebben oa betrekking op technische architectuur, beveiliging, functionaliteit, organisatie en procedures, bijv. de uitvoering van audits. Het afsprakenstelsel bevat onder meer onderdelen inzake informatiebeveiliging en privacy en incorporeert mede NEN-ISO/IEC 27002, BIR en VIR(BI). Vindplaats: www.afsprakenstelsel.etoegang.nl. Zie ook het Instellingsbesluit besturing elektronische toegangsdiensten, Strt. 2015 nr 10829.

Maatregelen
De voormalige gebruiksvoorwaarden bij de voorzieningen kenden tevens bepalingen die ten doel strekten om als overheid maatregelen te kunnen nemen op het moment dat er, de reeds getroffen maatregelen ten spijt, een aantasting of inbreuk op de (technische) beveiliging of de betrouwbaarheid van de processen plaatsvindt. Het gaat daarbij om het uitvoeren van onderhoud op de voorzieningen (periodieke software updates, aanpassingen tbv doorontwikkeling) en om het treffen van (nood)maatregelen om de beveiliging en betrouwbaarheid snel te herstellen als zich een incident of calamiteit voordoet en om (verdere) schade voor burgers en overheid te voorkomen. Hiertoe behoren eveneens maatregelen als het onderbreken of beëindigen van de toegang als gebruikers risico lopen cq slachtoffer zijn van (vermoed) misbruik van hun accounts. Het bovenstaande is thans in de regeling opgenomen.

Artikelsgewijs

Artikel 1

Voor de definities zal worden aangesloten bij het Besluit verwerking persoonsgegevens GDI, dat uitvoering zal geven aan het derde lid van artikel X van de wet.

Artikel 2

Dit artikel bevat de voor de gebruiker belangrijkste bepalingen uit de voormalige gebruiksvoorwaarden MijnOverheid: aangegeven wordt op welke wijze gebruik kan worden gemaakt van de voorziening MijnOverheid. Dit is een gepersonaliseerde elektronische voorziening waarmee voor burgers een persoonlijk domein beschikbaar komt dat geschikt is voor informatieverschaffing door overheidsorganen/afnemers en waardoor burgers hun post steeds vaker (uitsluitend) via het elektronische kanaal zullen ontvangen.
De gebruiksvoorwaarden zijn niet letterlijk overgenomen in de deze regeling. Bezien is welke gebruiksvoorwaarden geen plek in de regeling behoeven als gevolg van regulering elders. Zo wordt de verwerking van persoonsgegevens in het kader van het gebruik van MijnOverheid geregeld in het Besluit verwerking persoonsgegevens DigiD, DigiD Machtigen, MijnOverheid en BSN-Koppelregister. Voor wat betreft de rechtsgevolgen van het plaatsen van een bericht in de Berichtenbox is afdeling 2.3 van de Algemene wet bestuursrecht (Awb) van toepassing. Het sturen van notificaties (attenderingen) met betrekking tot plaatsing van berichten in de Berichtenbox naar het e-mailadres van een gebruiker, die hiervoor heeft gekozen bij activering van zijn MijnOverheid-account, is geen (onderdeel van de) bekendmaking in de zin van de Awb, maar een bestaande praktijk, die wordt gecontinueerd. Voorts zijn, bij gelegenheid van deze regeling, de bepalingen uit de voormalige gebruiksvoorwaarden geactualiseerd en gestroomlijnd. Werd in de gebruiksvoorwaarden bijvoorbeeld gesproken over het door de gebruiker “registreren” bij MijnOverheid, in de regeling wordt gesproken over “activeren”. Hiermee wordt het proces van ingebruikname accurater aangeduid.
MijnOverheid-accounts zullen standaard worden aangemaakt voor Nederlanders en ingezetenen vanaf 14 jaar. Reden hiervoor is dat dit de leeftijd is waarop men te maken krijgt met overheidsinstanties die voor het eerst (digitale) post toesturen; vanaf 14 jaar mag een jongere werken – en krijgt hij/zij dus te maken met de Belastingdienst – en vanaf die leeftijd geldt de identificatieplicht. In de nabije toekomst zal dus vanaf het 14e jaar voor ingezetenen en Nederlanders in het buitenland een account beschikbaar komen. Daarbij is niet langer sprake van het door gebruiker kunnen opzeggen of verwijderen van

het MijnOverheid-account. Beëindigen van het ontvangen van berichten van een of meerdere afnemers kan wel (lid 4), met uitzondering van de situatie waarin het gebruik van MijnOverheid wettelijk verplicht is gesteld (lid 5), zoals bijvoorbeeld bij de Belastingdienst (vide artikel I van de wet). De gebruiker kan zich te allen tijde weer elektronisch bereikbaar verklaren voor een of meerdere afnemers door deze opnieuw aan te vinken. Als een burger zijn MijnOverheid-account in gebruik heeft genomen, wordt er van hem verwacht dat hij de Berichtenbox regelmatig raadpleegt om te kijken of er nieuwe berichten zijn geplaatst. Ook wordt van hem verwacht dat hij, om notificaties te kunnen ontvangen, een actueel e-mailadres doorgeeft en ook een eventuele wijziging van dat adres.
Aangenomen moet worden dat het door de Minister opheffen van een MijnOverheid-account (lid 8) een besluit is in de zin van de Awb, gelet op het feit dat dit is gericht op rechtsgevolg. Immers: er kan dan niet langer gebruik gemaakt worden van de voorziening MijnOverheid, er kunnen geen berichten meer in de Berichtenbox geplaatst worden etc. Dat betekent dat bezwaar open staat bij de Minister van Binnenlandse Zaken en Koninkrijksrelaties, en daarna eventueel beroep bij de rechtbank en hoger beroep bij de Afdeling bestuursrechtspraak van de Raad van State.
Een uitgebreide procesbeschrijving, de door gebruiker te nemen stappen, vragen en antwoorden, nuttige adressen en telefoonnummers etc. zijn te vinden op mijn.overheid.nl.

Artikel 3

Dit artikel bevat de voor de gebruiker belangrijkste bepalingen uit de voormalige gebruiksvoorwaarden DigiD; aangegeven wordt op welke wijze gebruik kan worden gemaakt van DigiD.
De gebruiksvoorwaarden zijn niet letterlijk overgenomen in de onderhavige regeling. Bezien is welke bepalingen hier geen regulering behoeven als gevolg van het elders regelen van bepaalde onderdelen van de gebruiksvoorwaarden; zo zal de verwerking van persoonsgegevens in het kader van het gebruik van DigiD geregeld worden in het Besluit verwerking persoonsgegevens GDI. Ook zijn, bij gelegenheid van de onderhavige regeling, de bepalingen uit de voormalige gebruiksvoorwaarden geactualiseerd en gestroomlijnd.
Omdat de informatie, die gebruiker met DigiD bij de afnemers kan raadplegen, aanvragen en bewerken/wijzigen vaak privacygevoelig, vertrouwelijk en persoonlijk is, is het voor gebruiker van belang zijn DigiD strikt geheim te houden. Wanneer bij de gebruiker het vermoeden bestaat van identiteitsfraude, dan kan hij zijn DigiD laten blokkeren (opschorten) of opheffen. Dit kan via de Helpdesk (servicecentrum) van de dienst Logius (zie: www.digid.nl). Om weer diensten te kunnen afnemen bij afnemers, moet hij zijn DigiD laten deblokkeren respectievelijk een nieuwe DigiD aanvragen. Zie ook de toelichting bij artikel 7 (misbruik of oneigenlijk gebruik).
Een uitgebreide beschrijving van het aanvraagproces, de door gebruiker te nemen stappen, vragen en antwoorden, nuttige adressen en telefoonnummers etc. zijn te vinden op www.digid.nl en www.svb.nl.
Aangenomen moet worden, dat het toekennen (en dus ook: blokkeren en opheffen) van DigiD een besluit is in de zin van de Awb, gelet op het feit dat dit is gericht op rechtsgevolg. Immers: met dit authenticatiemiddel ('sleutel') wordt beoogd toegang te krijgen tot (onder meer) GDI-voorzieningen. Dat betekent dat bezwaar open staat bij de Minister van Binnenlandse Zaken en Koninkrijksrelaties, en daarna eventueel beroep bij de rechtbank en hoger beroep bij de Afdeling bestuursrechtspraak van de Raad van State.

Artikel 4

Dit artikel geeft aan wat de functie van het BSN-Koppelregister is: deze publieke voorziening legt een koppeling tussen een privaat authenticatiemiddel en het burgerservicenummer (bsn) van de gebruiker en controleert de identiteit van de gebruiker van het middel. Hierdoor wordt het gebruik van private authenticatiemiddelen in het publieke domein mogelijk. Voor de goede vervulling van deze – bij de Minister van Binnenlandse Zaken en Koninkrijksrelaties belegde – taak en teneinde de verificatie van de identiteit van gebruiker te kunnen uitvoeren, bevraagt het BSN-Koppelregister de Basisregistratie Personen.

Voorafgaand aan dit koppelproces maakt de gebruiker aan de private authenticatiedienst, van wie hij het desbetreffende authenticatiemiddel verkrijgt (bijv. een telecombedrijf of bedrijf dat digitale producten levert) kenbaar dat hij dit middel wil gebruiken voor de afname van diensten in het publieke domein, bijvoorbeeld voor het aanvragen van een vergunning of toeslag. De private authenticatiedienst die de mogelijkheid hiertoe biedt, schakelt vervolgens het BSN-Koppelregister in. De private authenticatiedienst levert hiertoe, met toestemming van de gebruiker, eenmalig een set persoonsgegevens aan bij het BSN-Koppelregister. Deze set bestaat uit (op basis van toestemming door gebruiker verkregen) naam, geboortedatum, het pseudo-ID op het authenticatiemiddel en (op basis van artikel X van de wet) het bsn. Terzake van het bsn dient de private authenticatiedienst een bewerkersovereenkomst te sluiten met de Minister als verantwoordelijke.
Nadat de initiële koppeling tussen privaat middel en bsn succesvol in het BSN-Koppelregister is geregistreerd, is het bsn voor het regulier inloggen bij de publieke dienstaanbieder niet meer nodig. Voor publieke dienstaanbieders (= afnemers van MijnOverheid cs) geldt dan, dat zij naast een publiek

authenticatiemiddel (DigiD) ook – via het BSN-Koppelregister gevalideerde – private authenticatiemiddelen moeten accepteren.
Benadrukt zij, dat sprake is van vrijwillige deelname in het kader van de introductie van het eID-stelsel. De tussenkomst van het BSN-Koppelregister is alleen relevant, indien de desbetreffende publieke dienstverlener en leverancier van private authenticatiemiddelen hebben aangegeven het gebruik van een privaat authenticatiemiddel in het publieke domein mogelijk te willen maken.
In het BSN-Koppelregister worden, zoals reeds aangegeven, persoonsgegevens verwerkt. De regels terzake worden opgenomen in het Besluit verwerking persoonsgegevens GDI.

Artikel 5

Niet alleen de direct betrokkene kan (via de GDI) zaken met de overheid regelen, dat kan ook een ander voor hem/haar doen. Dat kan door die ander, bijvoorbeeld een familielid of een zogenoemde Huba-medewerker (hulp bij aangifte inkomstenbelasting), te machtigen via DigiD Machtigen. Dit artikel bevat de voor de vertegenwoordigde en gemachtigde belangrijkste bepalingen uit de voormalige gebruiksvoorwaarden DigiD Machtigen; aangegeven wordt door wie en op welke wijze gebruik kan worden gemaakt van DigiD Machtigen. Voor de gemachtigde zijn ook de bepalingen met betrekking tot DigiD (artikel 3) relevant.
De gebruiksvoorwaarden zijn niet letterlijk overgenomen in de onderhavige regeling. Bezien is welke hun relevantie hebben verloren als gevolg van het elders regelen van bepaalde onderdelen van de gebruiksvoorwaarden; zo zal de verwerking van persoonsgegevens in het kader van het gebruik van DigiD Machtigen geregeld worden in het Besluit verwerking persoonsgegevens GDI. Ook zijn, bij gelegenheid van de onderhavige regeling, de bepalingen uit de voormalige gebruiksvoorwaarden geactualiseerd en gestroomlijnd.
Een uitgebreide procesbeschrijving, de door gebruiker te nemen stappen, vragen en antwoorden, nuttige adressen en telefoonnummers etc. zijn te vinden op www.digid.nl.
DigiD Machtiging biedt ook hulp aan niet-digitaalvaardige burgers, veelal vertegenwoordigden, die zelf geen gebruik kunnen maken van de website van DigiD Machtigen. Voor hen is er een telefonische Helpdesk waar een aanvraag voor of intrekking van een machtiging kan worden gedaan, of waar een schriftelijk overzicht met machtigingsaanvragen en machtigingen kan worden opgevraagd.

Artikel 6

Dit artikel betreft kaderstellende informatiebeveiliging en geeft aan welke normen worden gehanteerd om te komen tot een set (beveiligings)maatregelen om risico's het hoofd te kunnen bieden. Zie hetgeen hierover is opgemerkt in het algemeen deel onder punt 4.
Voor de volledigheid wordt opgemerkt, dat de veiligheid van de voorzieningen ook samenhangt met het gebruik dat er door afnemers van wordt gemaakt. Om die reden moeten ook afnemers, zoals gemeenten, aan diverse overheidsbrede voorschriften inzake informatiebeveiliging voldoen. Het toepasselijke kader behelst onder meer de Baselines informatieveiligheid en de normen en standaarden van de 'pas-toe-of-leg-uit-lijst', waaraan alle overheden zich via zelfregulering (programma's NUP en iNUP) hebben verbonden. Daarnaast moeten afnemers voldoen aan de contractvoorwaarden zoals die worden gehanteerd tussen de Minister van Binnenlandse Zaken en Koninkrijksrelaties (opdrachtnemer) en de afnemers (opdrachtgever/publieke dienstaanbieder). Deze relatie wordt gekenmerkt door een uitgebreide contractstructuur tussen Logius, de dienst digitale overheid van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, en (mede)overheden, in het kader van de levering van GDI-voorzieningen.
In het kader van informatiebeveiliging zijn met name de aansluitvoorwaarden relevant; dit zijn de voorschriften waaronder een afnemer kan aansluiten op de desbetreffende voorziening en waarmee hij moet instemmen als hij deze voorziening wil afnemen. Doel ervan is wederzijds duidelijkheid te scheppen over de verplichtingen waaraan zowel de afnemer als de Minister als beheerder van de voorziening moeten voldoen. Het betreft bijvoorbeeld de beveiligingseisen waaraan de afnemers – die verantwoordelijk zijn voor de beveiliging van hun eigen infrastructuur – moeten voldoen (oa het maken en naleven van veiligheidsplannen en het doen uitvoeren van audits), geheimhouding van te verwerken (indicatief opgesomde) gegevens door de afnemer, beheer en onderhoud. De meest actuele versies van de aansluitvoorwaarden zijn te vinden op www.logius.nl.

Artikel 7

Dit artikel betreft (re)actieve informatiebeveiliging, dat wil zeggen de maatregelen die zijn bedoeld om te kunnen handelen ingeval er, ondanks de eerder getroffen maatregelen, toch inbreuken of aantastingen op de voorzieningen optreden. Het artikel behelst het door de beheersorganisatie treffen van maatregelen bij beveiligingsincidenten, storingen en onderhoud en maatregelen bij misbruik of oneigenlijk gebruik. Teneinde de veiligheid en betrouwbaarheid van de voorzieningen te waarborgen en misbruik of oneigenlijk gebruik ervan zoveel mogelijk te voorkomen, is het nodig dit te kunnen signaleren en, bij constatering daarvan, adequaat te beëindigen.

Deze regeling voorziet in op dat moment te treffen maatregelen, om het (acute) risico weg te nemen. Gedacht kan worden aan het blokkeren (= opschorten) van een DigiD, het intrekken van een machtiging of het beëindigen van de toegang tot een MijnOverheid account.
In het kader van zijn beheerstaak kan de Minister controles uitvoeren op de gegevens die beschikbaar zijn binnen de voorzieningen, om concrete maatregelen te kunnen treffen.[1] Zo kunnen ongebruikelijke patronen worden onderkend die mogelijk duiden op misbruik of oneigenlijk gebruik. Ook kan gecontroleerd worden of gebruikers geen slachtoffer worden van reeds bekende, dwz zich eerder voorgedane, vormen van misbruik van de voorziening. Bij (het vermoeden van) misbruik of oneigenlijk gebruik, bijvoorbeeld het al dan niet met instemming van de rechtmatige eigenaar door een ander gebruiken van een DigiD activeringscode, hetgeen in strijd is met artikel 3 van deze regeling, kan de voorziening (al dan niet tijdelijk) worden geblokkeerd. De gebruiker wordt dan uitgesloten van toegang en verder gebruik van de voorziening.
Bij het BSN-Koppelregister, waar controle plaatsvindt op de unieke match tussen BSN en de andere aangeleverde persoonsgegevens, de geldigheid van het gebruikte identificatiedocument en de geldigheid van het private authenticatiemiddel, heeft eea tot gevolg dat een aangevraagde koppeling niet tot stand wordt gebracht of een tot stand gebrachte koppeling wordt beëindigd en de private authenticatiedienst terzake van het desbetreffende authenticatiemiddel geen gebruik (meer) van het BSN-Koppelregister kan maken cq het middel niet (langer) bruikbaar is in het publieke domein.
Bedacht moet worden dat artikel X van de wet betrekking heeft op de inrichting, beschikbaarstelling, instandhouding, werking, beveiliging en betrouwbaarheid van de bedoelde GDI-voorzieningen. Deze zorgplicht, die zich vertaalt in de geschetste beheersmaatregelen, is in het bijzonder van belang ter bescherming van de belangen van burgers; zij hebben immers recht op goede – digitale – dienstverlening door de overheid. Dat betekent dat zij ingeval van problemen, die verband houden met de voorzieningen, geholpen moeten en kunnen worden.
Het bovenstaande betekent, dat de (beheers)taak ook haar grens kent. Wanneer bijvoorbeeld een burger met gebruik van zijn DigiD overeenkomstig de bepalingen van art. 3 een frauduleuze aanvraag voor toeslagen indient, door bewust verkeerde posten in te vullen om meer toeslag te verkrijgen dan waar hij recht op heeft, is er geen sprake van aantasting van de betrouwbaarheid van de voorzieningen. Het is immers de burger die misbruik pleegt, met andere woorden het gebruik van de voorziening is frauduleus. In dat geval bestaat voor Logius geen wettelijke grondslag om uit eigen beweging dergelijke (vermoedens van) fraude te onderzoeken en hiervan melding te doen aan betrokken bestuursorganen. Tot de beheerstaak behoort, onverminderd artikel 162 van het Wetboek van Strafvordering, niet de opsporing ten behoeve van strafvorderlijke vervolging. Politie, justitie en daartoe bevoegde afnemers, zoals de Belastingdienst, kunnen aan Logius om informatie en gebruik(er)sgegevens verzoeken. Alsdan zal de relevante informatie worden aangeleverd overeenkomstig de daarvoor geldende wettelijke kaders.
Ook binnen het BSN-Koppelregister is ten behoeve van het operationeel beheer (goede werking, probleemanalyse etc.) sprake van (technische) controlemaatregelen met betrekking tot persoonsgegevens en digitale identiteit, logging en het bijhouden van een audittrail, waaruit op verzoek van politie en justitie gegevens opgeleverd kunnen worden, bijvoorbeeld over (afwijkend) gedrag van private authenticatiediensten.

Artikel 8

Gelet op aard en inhoud van deze regeling, is het niet opportuun om het Besluit inzake de vaststelling van de aansluitvoorwaarden en gebruiksvoorwaarden MijnOverheid (Scrt. 2007, 249) langer te handhaven. Dit besluit is bij de start van de website MijnOverheid.nl als proef, vastgesteld om afnemers en gebruikers transparantie te bieden. Destijds, en binnen die context, is toen vooralsnog gekozen voor het instrument van een ministerieel besluit dat afnemers en gebruikers duidelijkheid moest verschaffen over de te hanteren contractsvoorwaarden. Het ligt thans in de rede om dit besluit in te trekken. De gebruiksvoorwaarden gaan op in de deze regeling. De aansluitvoorwaarden zijn en blijven, zoals ook bij artikel 6 is aangegeven, van belang in de contractsrelatie tussen de Minister en de afnemer van de voorziening en zijn mede kenbaar en raadpleegbaar via de website van Logius.
Ook het Besluit persoonlijke internetpagina (Scrt. 2007, 102) waarin de zorgplicht van de Minister voor de voorloper van de voorziening MijnOverheid (Persoonlijke Internetpagina) is opgenomen, dient te vervallen. Artikel X, eerste lid, van de wet Elektronisch Berichtenverkeer verankert immers nu de zorg voor voorzieningen voor elektronisch berichtenverkeer en informatieverschaffing. Tenslotte is ook het Besluit beheer DigiD (Scrt. 2006, 160) overbodig geworden, nu de zorgplicht van de Minister voor de in dat besluit opgenomen overheidstoegangsvoorziening DigiD is opgegaan in de zorgplicht voor voorzieningen voor elektronische authenticatie als bedoeld in artikel X, eerste lid, van de wet Elektronisch Berichtenverkeer.

[1] In het kader van privacybescherming is met betrekking tot de te verwerken persoonsgegevens, de bijbehorende bewaartermijnen en aan wie deze gegevens mogen worden verstrekt, het toekomstige Besluit verwerking persoonsgegevens GDI van toepassing.

Artikel 9

De inwerkingtreding per 1 november 2015 is gekoppeld aan de inwerkingtreding van de wet. Deze kent een zekere spoedeisendheid, zoals aangegeven in de Memorie van Toelichting bij artikel XI van de wet.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
R.H.A. Plasterk