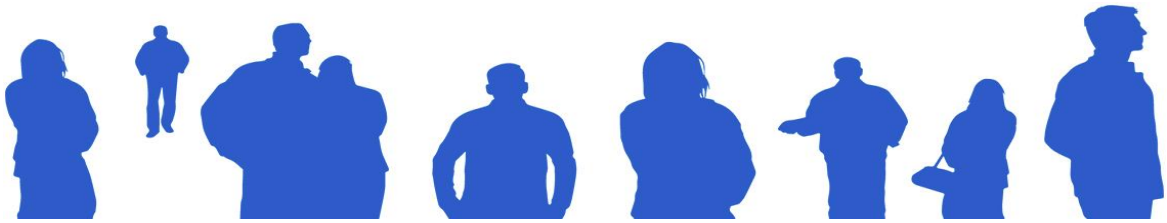


Identificatie/authenticatie in de BRP en de toepassing ervan bij bewerkersconstructies

Ministerie van BZK
Operatie BRP
Turfmarkt 147
2511 DC Den Haag

Contactpersoon:

Datum
13 januari 2015

Notitie

Inhoudsopgave

1. Doel

Doel van deze notitie is het in kaart brengen van de authenticatie/identificatie aspecten die verbonden zijn aan het systematisch verstrekken van gegevens uit de BRP aan daartoe geautoriseerde overheidsorganen en derden (i.v.m. de leesbaarheid in deze notitie aangeduid als afnemers) , die daarbij gebruikmaken van intermediairs.

2. Inleiding

Deze notitie is gebaseerd op de notitie 'juridische en beleidsmatige aspecten bewerkersconstructies (adm kantoren SNG TT)', opgesteld door BZK/B&I, afgestemd en van akkoord voorzien door het Afstemoverleg BRP waarin vertegenwoordigd zijn: Agentschap BPR, oBRP, BZK/CZW en BZK/B&I. In deze notitie zijn drie bewerkersconstructies voorzien van een aanvullende uitleg op de in de Ontwerpaspecten opgenomen teksten. Deze teksten geven een toelichting op hetgeen hierover in de wet- en regelgeving BRP is opgenomen.

1. Administratiekantoren met taken t.b.v. anderen (pensioenfondsen)
2. Stichting Netwerk Gerechtsdeurwaarders (SNG)
3. Bewerkers die alleen gegevens routeren (T&T)

In alle gevallen moet bij het verstrekken van gegevens uit de BRP door tussenkomst van bewerkers voldaan zijn aan de uitgangspunten in de wet- en regelgeving en beleidsuitgangspunten voor wat betreft de identificatie van de juridisch geautoriseerde partij en de authenticatie van de bevraging, levering en bijhouding.

Operatie BRP heeft voor de technische uitwerking van de identificatie en authenticatie in de BRP een voorstel gedaan in de memo 'Authenticatie Partijen'. Dit voorstel is afgestemd en van akkoord voorzien door het Afstemoverleg, de gedelegeerd opdrachtgever Operatie BRP heeft besloten akkoord te gaan met het voorstel en vervolgens opdracht te geven voor het opstellen van een globaal ontwerp. De memo is op 19 september 2014 in het ADM van het agentschap besproken en positief ontvangen.

In de notitie die voor ligt, wordt in hoofdstuk 3 een nadere uitleg gegeven van de technische oplossingsrichting van identificatie en authenticatie gebaseerd op de memo 'Authenticatie Partijen'.

Om als Afnemer te kunnen bepalen op welke wijze identificatie en authenticatie voor de eigen aansluiting(en) geregeld moet worden, is het type aansluiting van belang en de manier waarop de communicatie in technische zin met de BRP tot stand komt. In hoofdstuk 4 zijn de verschillende situaties in kaart gebracht en toegelicht.

In hoofdstuk 5 staan de hierboven genoemde drie bewerkersconstructies centraal. De informatie over de juridische en beleidsmatige aspecten is overgenomen uit de eerder genoemde notitie 'juridische en beleidsmatige aspecten bewerkersconstructies (adm kantoren SNG TT). Per constructie is nu ook een uitleg opgenomen over de toepassing van identificatie en authenticatie in de BRP.

Hoewel Bijhouders, in het kader van de samenwerkingsverbanden en/of andere bewerkersconstructies, ook gehouden zijn aan de voorschriften inzake authenticatie en identificatie wordt in deze notitie hier verder niet op ingegaan. Deze notitie is bedoeld voor de zogenaamde bewerkersconstructies die van toepassing zijn voor Afnemers.

3. Authenticatie van Partijen, de oplossingsrichting toegelicht

De BRP ontvangt en levert uitsluitend berichten van en aan juridisch geautoriseerde afnemers. Afnemers kunnen rechtstreeks communiceren met de BRP. In dat geval zijn deze Partijen direct aangesloten op de BRP. Afnemers kunnen er ook voor kiezen om een Bewerker in te schakelen in de communicatie met de BRP. In dat geval machtigt een Afnemer deze Bewerker om namens hem te communiceren met de BRP. Een gemachtigde bewerker wordt in dat geval ook als Partij geregistreerd in de BRP.

3.1 Communicatie & rollen in de BRP

Communicatie tussen de BRP en de Partijen volgt de Digikoppeling 3.0 standaard. Binnen deze standaard is gedefinieerd dat partijen zich identificeren met PKIO-certificaten. Hierbij wordt onderscheid gemaakt in:

- Certificaten voor de versleuteling (encryptie) van de communicatie;
- Certificaten voor de ondertekening (signing) van het bericht.

Voor wat betreft de berichtuitwisseling zelf wordt in de uitwerking van de oplossingsrichting onderscheid gemaakt tussen de volgende vormen van communicatie:

- *Synchrone communicatie*
  De Afnemer/Bewerker doet een verzoek aan de BRP ('request-response'-berichten zoals bevraging, bijhouding). Voor deze vorm van communicatie moet voldaan worden aan het Digikoppeling-profiel: '2W-be-S', WUS met 2 zijdige TLS + met signing;
- *Asynchrone communicatie*[1]
  De centrale voorziening BRP informeert de Afnemer/Bewerker ('push'-berichten zoals mutatie- en vulberichten, notificaties). Voor deze vorm van communicatie moet voldaan worden aan het Digikoppeling-profiel: '2W-R-S', WSRM (reliable messaging) met signing.

Vóór aansluiting op de BRP moeten IP-adressen uitgewisseld worden:

- Een Afnemer of Bewerker dient aan te geven met welke IP-adressen gecommuniceerd wordt, zodat deze in de whitelist van de centrale voorzieningen BRP kunnen worden opgenomen. Voor de asycnhrone communicatie zal tevens het zogenaamde adres van de ontvangstservice (het zogenaamde endpoint) moeten worden opgegeven;
- Het Agentschap BPR geeft vervolgens de IP-adressen aan waarvandaan de berichten vanuit de centrale voorziening worden gecommuniceerd. Zo kan een Afnemer of Bewerker deze ook in de eigen whitelist opnemen.

In de communicatie met de BRP worden de volgende rollen onderkend:

1. De Transporteur; voor het opzetten van een versleutelde verbinding
2. De Ondertekenaar; voor het digitaal ondertekenen van berichten.

Indien een geautoriseerde partij een Bewerker inschakelt, worden de machtigingen voor invulling van deze rollen in de BRP geregistreerd.

3.2 Machtigingen in de BRP

Er is altijd een juridisch geautoriseerde afnemer waarvoor één of meer autorisatiebesluiten zijn vastgesteld. Dit is de Geautoriseerde Partij. Indien een Geautoriseerde Partij zelfstandig aansluit zet deze zelf een versleutelde verbinding met de BRP op en ondertekent zelf de berichten. De Afnemer vult daarmee zelf de rollen van Transporteur en Ondertekenaar in.

Indien een Geautoriseerde Partij een Bewerker inschakelt, machtigt de Geautoriseerde Partij deze bewerker voor de rol van Transporteur en/of Ondertekenaar.

Indien een Bewerker als Ondertekenaar wordt gemachtigd, dient deze partij apart te worden gemachtigd voor de Diensten binnen het koppelvlak Levering.

De Geautoriseerde Partij moet bij de beheerder van de BRP (Agentschap BPR) aangeven welke combinaties van Transport- en Ondertekeningmachtigingen bij een Bewerker zijn toegestaan. Machtigingen en de gemachtigde partijen worden binnen de BRP geregistreerd. Bij het opzetten van de communicatie en de verwerking van binnenkomende berichten valideert de BRP of sprake is van een geldig PKIO-certificaat en een geldige machtiging.

Een Geautoriseerde Partij kan één of meer bewerkers machtigen om namens hem op te treden als Transporteur of Ondertekenaar. De specifieke rolverdeling is geen willekeurige keuze, maar is afhankelijk van de wijze waarop de Geautoriseerde Partij de aansluiting op de BRP regelt (zie hiervoor de toelichting in hoofdstuk 4. Inrichting identificatie & authenticatie per type aansluiting).

3.3 Identificatie in de BRP

Voor de identificatie van geregistreerde Partijen (Afnemers en Bewerkers) en machtigingen in de BRP wordt het OverheidsIdentificatieNummer (OIN) gebruikt. Dit OIN[2] is opgenomen in het PKIO-certificaat. Een Afnemer of Bewerker moet altijd zijn eigen PKIOverheid-certificaat inclusief unieke OIN gebruiken in de communicatie met de BRP. Een Geautoriseerde Partij stelt dus nooit zijn eigen PKIO-certificaat ter beschikking aan zijn gemachtigde bewerker.

In de BRP worden geen afzonderlijke certificaat-gegevens opgenomen. Nadat is vastgesteld dat het certificaat een geldig PKIO-certificaat is, gaat de voorgestelde oplossingsrichting er vanuit dat het in

[1] In de notitie van oBRP is ook het Digikoppeling-profiel "osb-rm-s" voor asynchrone berichten genoemd. Inmiddels heeft de Stuurgroep in oktober 2014 met vaststelling van het document 'Samenvatting scope Operatie BRP' vastgesteld dat voor de BRP geen gebruik gemaakt zal worden van eBMS. Dit profiel is daarom niet meer van toepassing.
[2] Een OIN wordt toegekend door Logius. Nadat het OIN is verkregen kan bij één van de aangewezen Certificatiedienstverleners (CSP's zijn: Digidentity, EAG, KPN en QuoVadis) een PKIO-certificaat worden aangevraagd.

het certificaat opgenomen OIN vertrouwd kan worden en vanaf dat moment in het proces gebruikt wordt voor de identificatie van de betreffende Partij in de verdere BRP-verwerking.

Sluit een Geautoriseerde Partij direct aan op de BRP en beschikt deze nog niet over een PKIO-certificaat met eigen OIN, dan vraagt de Geautoriseerde Partij zelf zijn PKIO-certificaat en OIN aan.

Indien een Geautoriseerde Partij zijn bewerker machtigt voor zowel de rol van Transporteur als van Ondertekenaar hoeft de Geautoriseerde Partij niet zelf een PKIO-certificaat en OIN aan te vragen ten behoeve van de communicatie met of de identificatie binnen de BRP. Dit moet zijn gemachtigde Bewerker doen.

De Geautoriseerde Partij blijft de eindverantwoordelijke voor de beveiliging van de gegevens bij bewerker(s), het transport tussen bewerkers en het transport tussen de geautoriseerde en een bewerker. De Geautoriseerde Partij kan deze eindverantwoordelijkheid niet contractueel verleggen naar een andere partij. Het wordt daarom sterk aanbevolen om de communicatie tussen de Geautoriseerde Partij en zijn Bewerker op een zelfde beveiligde manier tot stand te laten komen als de communicatie tussen de BRP en de Bewerker. Hierover maakt de Geautoriseerde Partij zelf afspraken met zijn Bewerker.

3.4 Authenticatie in de BRP

Met authenticatie wordt in de BRP geregeld dat altijd in juridische zin is te achterhalen welke Geautoriseerde Partij welke gegevens van wie heeft opgevraagd c.q. verstrekt heeft gekregen. Ook al heeft deze Geautoriseerde Partij voor de daadwerkelijke bevraging en levering een Bewerker ingeschakeld.

Binnen het koppelvlak Levering (Afnemers) moet in elk bericht van/naar de BRP in de stuurgegevens van het bericht de Partijcode van het juridisch geautoriseerde overheidsorgaan of derde zijn opgenomen als formele zender en ontvanger. Tevens moet de Abonnementnaam in de parameters zijn opgenomen. In geval van het plaatsen/ verwijderen van afnemersindicaties moet de Abonnementnaam in het bericht zelf zijn opgenomen. Met de Abonnementnaam wordt een relatie gelegd met de Diensten en Gegevens waarvoor een Geautoriseerde Partij *in juridische zin* geautoriseerd is, zoals dit is vastgelegd in het autorisatiebesluit.

In de BRP wordt de autorisatie voor Diensten en Gegevens vastgelegd in de vorm van één of meerdere Abonnementen. Een Geautoriseerde partij heeft vervolgens toegang tot één of meerdere van deze Abonnementen conform zijn autorisatiebesluit(en). In de communicatie met de BRP dient de Geautoriseerde partij op te geven op basis van welk Abonnement hij dit doet. Het abonnement wordt geïdentificeerd door de Abonnementnaam.

Als een Afnemer meerdere diensten afneemt waarbij de doelbindingspopulatie of de te leveren gegevens afwijken, dan moeten deze onder verschillende abonnementen worden ondergebracht. Een Afnemer die nu bijvoorbeeld ad hoc bevraging heeft en daarnaast afnemerindicaties mag plaatsen maar een kleinere set van rubrieken spontaan geleverd mag krijgen, zal in de BRP twee abonnementen krijgen: één voor ('ad hoc') zoeken en bevragen en één voor mutatielevering op basis van afnemerindicatie.

Ter verduidelijking: de manier waarop de term 'abonnement' in de BRP gebruikt wordt, is vergelijkbaar met de manier waarop deze term gehanteerd wordt door bijvoorbeeld telefoon providers: het is een contract/raamwerk waarbinnen diensten geleverd kunnen worden. Welke diensten dat precies zijn is per abonnement verschillend en kan ook in de tijd wijzigen[3].

3.5 Autorisatie in de BRP

Samengevat spelen de volgende gegevens een rol wat betreft de autorisatie in de BRP:

- De identiteit van de Ondertekenaar; deze wordt door de BRP vastgesteld op basis van de OIN van de Ondertekenaar;
- In geval van machtigingen controleert de BRP de geldigheid van deze machtiging(en);
- In de stuurgegevens van elk bericht is de Partijcode van de Geautoriseerde Partij opgenomen;
- In de parameters van elk bericht, of in geval van het plaatsen/verwijderen van afnemerindicaties in het bericht zelf, moet de Abonnementnaam zijn opgenomen.

3 De toelichting op de term Abonnement is afkomstig uit de BRP Dienstencatalogus t.b.v. afnemers, versie 1.1.0. Voor meer informatie wordt verwezen naar hoofdstuk 4 uit dit document.

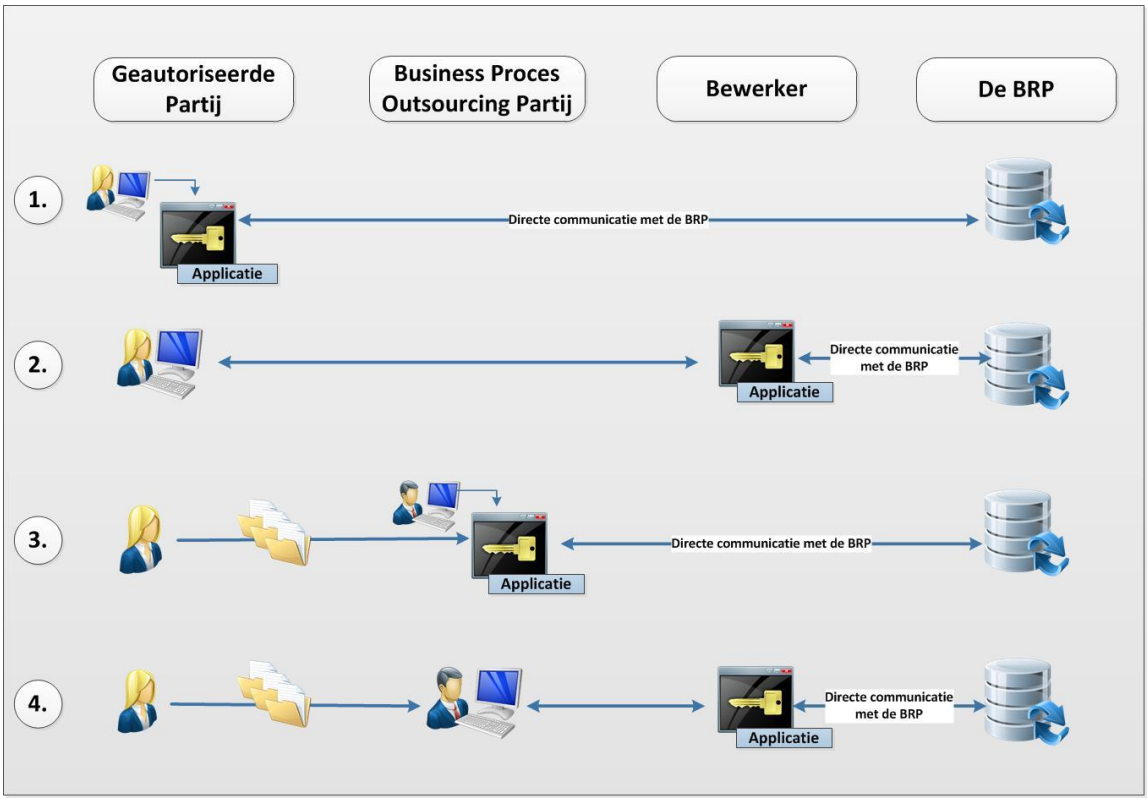
Indien een Geautoriseerde Partij voor de communicatie met de BRP een Bewerker heeft gemachtigd, dan dient deze Bewerker te beschikken over de Partijcode en Abonnementnaam van de Geautoriseerde Partij om in elk bericht aan de BRP op te kunnen nemen. De Geautoriseerde Partij blijft altijd *verantwoordelijk* voor het correct plaatsen van de Partijcode en de Abonnementnaam op berichten, ook al heeft hij voor de uitvoering ervan zijn Bewerker gemachtigd.

4. Inrichting identificatie & authenticatie per type aansluiting

De wijze waarop de identificatie en authenticatie per Geautoriseerde Partij geregeld moet worden, is afhankelijk van de manier waarop deze partij gaat aansluiten op de BRP in combinatie met:

1. De positionering van de applicatie van waaruit het bericht wordt opgesteld voor de bevraging van de BRP;
2. De positionering van de applicatie van waaruit de berichten naar de BRP worden verstuurd.

Dit levert – naar nu wordt aangenomen – vier mogelijke situaties op[4]. In de onderstaande figuur zijn deze mogelijkheden visueel weergegeven en per situatie nader toegelicht.



Een Geautoriseerde Partij kan in de communicatie met de BRP gebruik maken van 1 of meer type aansluitingen. Een Geautoriseerde Partij heeft altijd maar één Partijcode. Afhankelijk van diens autorisatiebesluit(en) kan een Geautoriseerde Partij één of meer Abonnementen hebben.

4 Indien in de praktijk blijkt dat er meer mogelijkheden zijn, dan worden deze in dit overzicht opgenomen en op een zelfde manier uitgewerkt.

4.1 Toelichting op de rollen

Geautoriseerde Partij	Dit is de partij die in *juridische* zin geautoriseerd is en dus één of meer autorisatiebesluiten heeft. Dit is de partij die wordt aangesloten op de BRP.
Business Proces Outsourcing Partij	Dit is een (commerciële) partij aan wie een Geautoriseerde Partij in meer of mindere mate zijn – administratieve – processen heeft uitbesteed. Deze BPO handelt namens één of meer Geautoriseerde Partijen. Deze BPO is nooit zelf in juridische zin geautoriseerd[5]. Indien een Geautoriseerde Partij naast de uitbesteding van processen, zijn BPO ook inzet voor de directe communicatie met de BRP, vervult de BPO in feite ook de rol van Bewerker.
Bewerker	Dit is een (commerciële) partij die een Geautoriseerde Partij inschakelt in de technische uitvoering voor de bevraging/levering van gegevens. Dit betekent dat *de applicatie van de bewerker* wordt gebruikt voor de directe communicatie met de BRP. Een Bewerker is nooit zelf in juridische zin geautoriseerd.
De BRP	Dit zijn de centrale BRP voorzieningen waarop alle Geautoriseerde Partijen aansluiten, al dan niet via een BPO of Bewerker.

4.2 Type aansluitingen i.r.t. identificatie en authenticatie

Situatie 1

De Geautoriseerde Partij sluit zowel in juridische als technische zin aan op de BRP.

De Geautoriseerde Partij sluit zelfstandig aan op de BRP en doet het werk en beheer van de applicatie die direct communiceert met de BRP 'in huis'. Dit kan betekenen dat een Geautoriseerde Partij zelfbouwer is, maar het kan ook zijn dat hij voor de ontwikkeling en implementatie van de applicatie een leverancier heeft ingeschakeld .

De Geautoriseerde Partij vult zelf de rollen van Transporteur en Ondertekenaar in en machtigt geen andere partijen.

De Geautoriseerde Partij zet zelf de versleutelde verbinding met de BRP op en ondertekent zelf de berichten met zijn eigen OIN. Dit OIN is opgenomen in het PKIO-certificaat van de Geautoriseerde Partij. Omdat de Geautoriseerde Partij direct communiceert met de BRP kan een en hetzelfde PKIOverheid-certificaat en OIN toegepast worden.

De Geautoriseerde Partij neemt in elk bericht aan de BRP zijn eigen Partijcode en de betreffende Abonnementnaam op.

Voor deze aansluiting is alleen de Geautoriseerde Partij als Partij in de BRP geregistreerd.

Situatie 2

De Geautoriseerde Partij sluit in juridische zin aan op de BRP.

De Geautoriseerde Partij maakt zowel voor het opstellen van berichten als het transport naar de BRP gebruik van de applicatie van de Bewerker. Met andere woorden, de directe communicatie met de BRP voor deze Geautoriseerde Partij komt vanuit de applicatie van de Bewerker tot stand. Het beheer van de applicatie is belegd bij deze Bewerker.

[5] In de huidige aansluiting op GBA-V heeft deze BPO namens de Geautoriseerde Partij(en) autorisatie verkregen voor de systematische verstrekking van gegevens uit de basisregistratie personen. Dit betekent dat de BPO een login en wachtwoord heeft voor toegang tot GBA-V en/of de GBA-mailboxserver. De BPO zorgt ervoor dat deze Geautoriseerde Partij(en) zijn gegevens conform het autorisatiebesluit geleverd krijgt via de login en wachtwoord van de BPO op GBA-V en/of GBA-mailboxserver. Met de BRP verdwijnt deze constructie met login en wachtwoord.

De Geautoriseerde Partij machtigt de Bewerker voor:

- de rol van Transporteur;
- de rol van Ondertekenaar;
- toegang tot de Diensten.

De Bewerker zet namens de Geautoriseerde Partij de versleutelde verbinding met de BRP op en ondertekent de berichten met zijn eigen OIN. Dit OIN is opgenomen in het PKIO-certificaat van de Bewerker. Indien de Bewerker een private partij is, kan deze een op het KvK nummer gebaseerd OIN toegewezen krijgen.

De Geautoriseerde Partij is verantwoordelijk voor het aanleveren van zijn Partijcode en de Abonnementnaam aan de Bewerker voor het correct samenstellen van berichten aan de BRP.

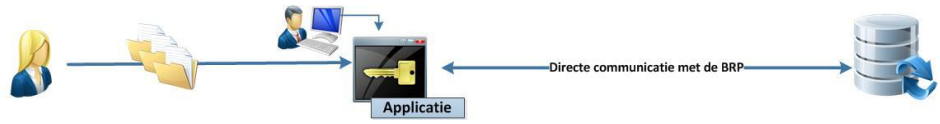
De Bewerker neemt in elk bericht aan de BRP de Partijcode van de Geautoriseerde Partij door wie hij gemachtigd is en de betreffende Abonnementnaam op.

Indien een Bewerker namens meer dan één Geautoriseerde Partij direct communiceert met de BRP wordt door de Bewerker een en hetzelfde PKIO-certificaat en OIN gebruikt. Elke Geautoriseerde Partij moet deze Bewerker via de beheerder van de BRP (Agentschap BPR) separaat machtigen.

Door het opnemen van de Partijcode van de Geautoriseerde Partij en de Abonnementnaam in de stuurgegevens van de berichten door de Bewerker is altijd te herleiden namens welke Geautoriseerde Partij de BRP is bevraagd c.q. aan welke Geautoriseerde Partij is verstrekt.

Voor deze aansluiting zijn de Geautoriseerde Partij en de gemachtigde Bewerker als Partij in de BRP geregistreerd.

Situatie 3



De Geautoriseerde Partij sluit in juridische zin aan op de BRP. De Geautoriseerde Partij besteedt in meer of mindere mate zijn – administratieve - processen uit aan een BPO.

De Geautoriseerde Partij maakt zowel voor het opstellen van berichten als het transport naar de BRP gebruik van de applicatie van de BPO. Met andere woorden, de directe communicatie met de BRP voor deze Geautoriseerde Partij komt vanuit de applicatie van de BPO tot stand. Het beheer van de applicatie is belegd bij de BPO. Dit kan betekenen dat de BPO zelfbouwer is, maar het kan ook zijn dat hij voor de ontwikkeling en implementatie van de applicatie een leverancier heeft ingeschakeld.

De Geautoriseerde Partij machtigt de BPO voor:

- de rol van Transporteur;
- de rol van Ondertekenaar;
- toegang tot de Diensten.

De BPO zet namens de Geautoriseerde Partij de versleutelde verbinding met de BRP op en ondertekent de berichten met zijn eigen OIN. Dit OIN is opgenomen in het PKIO-certificaat van de BPO. Indien de BPO een private partij is, kan deze een op het KvK nummer gebaseerd OIN toegewezen krijgen.

De Geautoriseerde Partij is verantwoordelijk voor het aanleveren van zijn Partijcode en de Abonnementnaam aan de BPO voor het correct samenstellen van berichten aan de BRP. In de daadwerkelijke uitvoering kan de Geautoriseerde Partij dit hebben uitbesteed aan zijn BPO. De Geautoriseerde Partij blijft echter altijd verantwoordelijk.

De BPO neemt in elk bericht aan de BRP de Partijcode van de Geautoriseerde Partij door wie hij gemachtigd is en de betreffende Abonnementnaam op.

Indien een BPO namens meer dan één Geautoriseerde Partij direct communiceert met de BRP wordt door de BPO een en hetzelfde PKIO-certificaat en OIN gebruikt. Elke Geautoriseerde Partij moet deze BPO via de beheerder van de BRP (Agentschap BPR) separaat machtigen.

Door het opnemen van de Partijcode van de Geautoriseerde Partij en de Abonnementnaam in de stuurgegevens van de berichten door de Bewerker is altijd te herleiden namens welke Geautoriseerde Partij de BRP is bevraagd c.q. aan welke Geautoriseerde Partij is verstrekt.

Voor deze aansluiting zijn de Geautoriseerde Partij en de gemachtigde BPO als Partij in de BRP geregistreerd.

In deze situatie heeft een Geautoriseerde Partij de uitvoering van – administratieve – processen aan zijn BPO uitbesteed en maakt hij gebruik van de applicatie van de BPO in de directe communicatie met de BRP. Strikt genomen fungeert de BPO voor zijn Geautoriseerde Partij(en) in deze situatie zowel als BPO (in de uitvoering van processen) als Bewerker (in de technische uitvoering van de directe communicatie met de BRP).

Situatie 4

De Geautoriseerde Partij sluit in juridische zin aan op de BRP. De Geautoriseerde Partij besteedt in meer of mindere mate zijn – administratieve - processen uit aan een BPO.

De Geautoriseerde Partij maakt via de BPO zowel voor het opstellen van berichten als het transport naar de BRP gebruik van de applicatie van de Bewerker. Met andere woorden, de directe communicatie met de BRP voor deze Geautoriseerde Partij komt vanuit de applicatie van de Bewerker tot stand. Het beheer van de applicatie is belegd bij deze Bewerker.

De Geautoriseerde Partij machtigt de Bewerker voor:

- de rol van Transporteur;
- de rol van Ondertekenaar;
- toegang tot de Diensten.

De Bewerker zet namens de Geautoriseerde Partij de versleutelde verbinding met de BRP op en ondertekent de berichten met zijn eigen OIN. Dit OIN is opgenomen in het PKIO-certificaat van de Bewerker. Indien de Bewerker een private partij is, kan deze een op het KvK nummer gebaseerd OIN toegewezen krijgen.

De Geautoriseerde Partij is verantwoordelijk voor het aanleveren van zijn Partijcode en de Abonnementnaam aan de Bewerker voor het correct samenstellen van berichten aan de BRP. In de daadwerkelijke uitvoering kan de Geautoriseerde Partij dit hebben uitbesteed aan zijn BPO. De Geautoriseerde Partij blijft echter altijd verantwoordelijk.

De Bewerker neemt in elk bericht aan de BRP de Partijcode van de Geautoriseerde Partij door wie hij gemachtigd is en de betreffende Abonnementnaam op.

Indien een Bewerker namens meer dan één Geautoriseerde Partij direct communiceert met de BRP wordt door de Bewerker een en hetzelfde PKIO-certificaat en OIN gebruikt. Elke Geautoriseerde Partij moet deze Bewerker via de beheerder van de BRP (Agentschap BPR) separaat machtigen.

Door het opnemen van de Partijcode van de Geautoriseerde Partij en de Abonnementnaam in de stuurgegevens van de berichten door de Bewerker is altijd te herleiden namens welke Geautoriseerde Partij de BRP is bevraagd c.q. aan welke Geautoriseerde Partij is verstrekt.

Voor deze aansluiting zijn de Geautoriseerde Partij en de gemachtigde Bewerker als Partij in de BRP geregistreerd. Dit betekent dat de BPO niet als Partij geregistreerd wordt in de BRP. De BPO behoudt wel zijn functie in de uitvoering van processen namens zijn Geautoriseerde Partij(en), tenzij een Geautoriseerde Partij daarover andere afspraken maakt. Ook kan deze BPO als contactpersoon of coördinerend orgaan blijven optreden voor het Agentschap BPR in de communicatie met zijn Geautoriseerde Partij(en).

4.3 Bepalen van eigen situatie o.b.v. type aansluiting op de BRP

Een Geautoriseerde Partij die voor zijn aansluiting moet beoordelen welke situatie voor hem van toepassing is, moet uitgaan van de situatie zoals hij voornemens is aan te sluiten op de BRP tenzij een afnemer hierin geen wijzigingen wenst aan te brengen ten opzichte van zijn huidige GBA-V aansluiting.

Voorbeeld: voor een Geautoriseerde Partij is in de huidige aansluiting op GBA-V de hierboven beschreven situatie 2 van toepassing. Deze Geautoriseerde Partij is echter van plan om direct op de BRP aan te gaan sluiten waardoor situatie 1 van toepassing wordt. Om te bepalen wie wat moet doen in het kader van de aansluiting op de BRP moet deze Geautoriseerde Partij de werkwijze onder situatie 1 volgen.

5. De bewerkersconstructies

De tekst in dit hoofdstuk over de bewerkersconstructies is wat betreft de *juridische en beleidsmatige aspecten* overgenomen uit de notitie 'juridische en beleidsmatige aspecten bewerkersconstructies (adm kantoren SNG TT)'. Per bewerkersconstructie is in deze notitie een paragraaf toegevoegd met een uitleg over de *toepassing van identificatie en authenticatie* in de BRP.

5.1 Administratiekantoren met taken t.b.v. anderen (pensioenfondsen)

5.1.1 Juridische en beleidsmatige aspecten

Onderstaande tekst is overgenomen uit de notitie 'juridische en beleidsmatige aspecten bewerkersconstructies (adm kantoren SNG TT)':

"Administratiekantoren kunnen worden aangemerkt als bewerker van gegevens namens de pensioenfondsen die van hun diensten gebruik maken. In de ontwerpaspecten is geconcludeerd dat de binnen deze kantoren gehanteerde werkwijze beschouwd kan worden als het verstrekken van gegevens door pensioenfonds A aan pensioenfonds B. Deze verstrekking van gegevens vindt plaats onder de Wbp en niet onder de Wet BRP. In juridische zin is voor de uitvoering van de Wet BRP slechts relevant dat het pensioenfonds namens wie door het administratiekantoor gegevens over een ingeschrevene worden opgevraagd, een relatie heeft met de betrokken persoon en daardoor geautoriseerd is om de bevraging te (laten) doen. De daaruit voortvloeiende verstrekking aan dat pensioenfonds wordt in de BRP geprotocolleerd. In juridische BRP termen is dat pensioenfonds de partij waaraan wordt versterkt. De verstrekking van de uit de BRP verkregen gegevens (die in juridische zin dan geen BRP-gegevens meer zijn) door het desbetreffende pensioenfonds aan andere pensioenfondsen (via het administratiekantoor als bewerker) valt onder de Wbp. Het toezicht op deze nadere gegevensverwerking onder de Wbp berust bij het CBP.

De vraag die hierbij gesteld kan worden is of met deze werkwijze voldaan wordt aan de in het privacyrecht relevante transparantievereisten voor gegevensverwerkingen, i.c. de verwerking van gegevens in de BRP. Een burger die bv. een brief ontvangt van pensioenfonds C ziet in zijn protocolleringsgegevens dat alleen voor pensioenfonds A gegevens uit de BRP zijn opgevraagd. Dat er daarna nog een verstrekking van zijn gegevens onder de Wbp heeft plaatsgevonden door pensioenfonds A aan pensioenfonds C wordt in de BRP niet geprotocolleerd.

Het valt niet te ontkennen dat er voor de ingeschrevene een grotere transparantie ontstaat met betrekking tot de verstrekking van hem betreffende gegevens uit de BRP aan pensioenfondsen, indien iedere verstrekking aan ieder pensioenfonds individueel in de BRP zou worden geprotocolleerd. Dat veronderstelt dat iedere bevraging dan ook door (of namens) ieder pensioenfonds wordt gedaan. Hoewel een dergelijke opzet wenselijk zou zijn en nagestreefd dient te worden, wordt echter op zich aan de vereiste transparantie van de gegevensverwerking in de BRP voldaan, indien in het hierboven genoemde voorbeeld de verstrekking van gegevens over een ingeschrevene aan pensioenfonds A wordt geprotocolleerd. De pensioenfondsen zijn zelf verantwoordelijk voor de op grond van de Wbp vereiste transparantie betreffende verstrekkingen binnen de administratiekantoren."

5.1.2 Inrichting identificatie & authenticatie

Voor de administratiekantoren kan in de aansluiting op de BRP situatie 3 of situatie 4 van toepassing zijn. Dit is afhankelijk van de manier waarop de technische aansluiting is geregeld.

Administratiekantoor/pensioenfondsen sluiten volgens <u>situatie 3</u> aan op de BRP	
Geautoriseerde Partij	Het Pensioenfonds
BPO Let op: de BPO fungeert in deze situatie ook als Bewerker	Het Administratiekantoor Het Administratiekantoor voert **in de rol van BPO** de – administratieve – processen uit namens zijn Pensioenfonds(en)
Bewerker	Het Administratiekantoor Het Administratiekantoor gebruikt **in de rol van Bewerker** zijn eigen applicatie voor de directe communicatie met de BRP namens zijn Pensioenfonds(en).
Machtiging	Pensioenfonds machtigt het Administratiekantoor (in de rol van Bewerker) voor:

Administratiekantoor/pensioenfondsen sluiten volgens <u>situatie 3</u> aan op de BRP	
	• rol van Transporteur • rol van Ondertekenaar • toegang tot Diensten
Identificatie	PKIO-certificaat en OIN van het Administratiekantoor
Authenticatie	Formeel levert het Pensioenfonds aan het Administratiekantoor (in de rol van Bewerker) t.b.v. het samenstellen van berichten aan de BRP: • de partijcode van het Pensioenfonds • met de bijbehorende Abonnementnaam Het Pensioenfonds is hiervoor verantwoordelijk, maar heeft de uitvoering ervan uitbesteed aan zijn Administratiekantoor (in de rol van BPO).
Partijen in BRP	Het Pensioenfonds en het Administratiekantoor worden voor die aansluiting als Partijen geregistreerd in de BRP.

Administratiekantoor/pensioenfondsen sluiten volgens <u>situatie 4</u> aan op de BRP	
Geautoriseerde Partij	Het Pensioenfonds
BPO	Het Administratiekantoor
Bewerker	<Naam Bewerker>[6]
Machtiging	Pensioenfonds machtigt de Bewerker voor: • rol van Transporteur • rol van Ondertekenaar • toegang tot Diensten
Identificatie	PKIO-certificaat en OIN van de Bewerker
Authenticatie	Formeel levert het Pensioenfonds aan de Bewerker t.b.v. het samenstellen van berichten aan de BRP: • de partijcode van het Pensioenfonds • met de bijbehorende Abonnementnaam Het Pensioenfonds is hiervoor verantwoordelijk, maar heeft de uitvoering ervan uitbesteed aan zijn Administratiekantoor. In de praktijk zal de Bewerker deze gegevens via het Administratiekantoor aangeleverd krijgen.
Partijen in BRP	Het Pensioenfonds en de Bewerker worden voor die aansluiting als partijen geregistreerd in de communicatie met de BRP. **Let op**: het Administratiekantoor wordt voor deze aansluiting dus **niet** als Partij geregistreerd in de BRP. Het Administratiekantoor kan als BPO wel zijn functie behouden in de uitvoering van processen namens zijn Pensioenfonds(en). Ook kan het Administratiekantoor als contactpersoon of coördinerend orgaan blijven optreden voor het Agentschap BPR in de communicatie met zijn Pensioenfonds(en).

5.2 Stichting Netwerk Gerechtsdeurwaarders (SNG)

5.2.1 Juridische en beleidsmatige aspecten

Onderstaande tekst is overgenomen uit de notitie 'juridische en beleidsmatige aspecten bewerkersconstructies (adm kantoren SNG TT)':

"De huidige manier van werken van de SNG is niet in overeenstemming met de Wet BRP en was dat ook al niet onder de Wet GBA. Uit de BRP dient te blijken aan welke individuele deurwaarder gegevens over een bepaalde persoon zijn verstrekt. Dit betekent dat iedere deurwaarder rechtsreeks als Geautoriseerde Partij in de technische systemen van de BRP dient te worden opgenomen, zodat de gegevensverstrekking aan de betrokken deurwaarder kan worden geprotocolleerd. Voorts dient te worden voldaan aan de uitgangspunten van de Ontwerpaspecten BRP wat betreft de identificatie en authenticatie bij de verstrekking van gegevens aan een partij, indien deze verstrekking plaatsvindt door tussenkomst van een bewerker."

[6] In de huidige aansluiting op GBA-V wordt door pensioenfondsen/administratiekantoren gebruik gemaakt van T&T als Bewerker.

5.2.2 Inrichting identificatie & authenticatie

Voor SNG en de gerechtsdeurwaarders is situatie 3 van toepassing in de aansluiting op de BRP.

SNG/Gerechtsdeurwaarders sluiten volgens <u>situatie 3</u> aan op de BRP	
Geautoriseerde Partij	De Gerechtsdeurwaarder
BPO Let op: de BPO fungeert in deze situatie ook als Bewerker	SNG SNG voert **in de rol van BPO** de – administratieve – processen uit namens zijn Gerechtsdeurwaarders.
Bewerker	SNG SNG gebruikt **in de rol van Bewerker** zijn eigen applicatie voor de directe communicatie met de BRP namens zijn Gerechtsdeurwaarders.
Machtiging	Gerechtsdeurwaarder machtigt SNG (in de rol van Bewerker) voor: • rol van Transporteur • rol van Ondertekenaar • toegang tot Diensten
Identificatie	PKIO-certificaat en OIN van SNG
Authenticatie	De Gerechtsdeurwaarder levert aan SNG (in de rol van Bewerker) t.b.v. het samenstellen van berichten aan de BRP: • de partijcode van de Gerechtsdeurwaarder • met de bijbehorende Abonnementnaam
Partijen in BRP	De Gerechtsdeurwaarder en SNG worden voor die aansluiting als Partijen geregistreerd in de BRP.

5.3 Bewerkers die gegevens alleen routeren (T&T)[7]

5.3.1 Juridische en beleidsmatige aspecten

De positie van deze bewerkers wijkt in wezen niet af van die van de SNG en pensioenfondsen. Dit betekent dat ook voor verstrekkingen die via deze bewerkers lopen het noodzakelijk is om in de BRP te kunnen vastleggen wie de Geautoriseerde Partij (en dus de verantwoordelijke) is voor de verwerking van de uit de BRP verstrekte gegevens. Indien voor de identificatie geen gebruik wordt gemaakt van een digitale handtekening, dient conform de Ontwerpaspecten BRP de manier van werken zodanig te zijn, dat de gegevensverstrekking uit de BRP over een bepaalde persoon aan een individuele juridisch geautoriseerde afnemer rechtstreeks in de BRP kan worden vastgelegd. Daarnaast moet ook op het punt van de authenticatie aan de uitgangspunten van de Ontwerpaspecten BRP worden voldaan. Dit betekent dat authenticatie dient plaats te vinden van de geautoriseerde afnemers (partijen) en van de bewerker om te controleren of de gegevens worden gevraagd in overeenstemming met de juridische autorisatie.

5.3.2 Inrichting identificatie & authenticatie

Een Geautoriseerde Partij maakt in de aansluiting op de BRP conform situatie 2 en 4 gebruik van dit type Bewerker. In de naam van deze constructie is alleen T&T opgenomen. Er zijn echter meer Bewerkers die door een Geautoriseerde Partij kunnen worden ingeschakeld zoals BKWI, Centric, PinkRoccade of Procura.

Voor een uitwerking van situatie 4 wordt verwezen naar §5.1.2. Onderstaand de uitwerking van de rolverdeling in situatie 2.

[7] De naamgeving van dit type constructie is afkomstig uit de oorspronkelijke notitie van B&I, maar dekt feitelijk niet (volledig) de lading. Het gaat hier om bewerkers wiens applicatie nu gebruikt wordt voor het opzetten van de directe communicatie met GBA-V (en straks voor de BRP). Dus zowel voor het opstellen van een bericht als het transport ervan.

Geautoriseerde Partij sluit volgens <u>situatie 2</u> aan op de BRP	
Geautoriseerde Partij	<Geautoriseerde Partij>
BPO	Niet van toepassing
Bewerker	<Naam Bewerker>
Machtiging	Geautoriseerde Partij machtigt de Bewerker voor: • rol van Transporteur • rol van Ondertekenaar • toegang tot Diensten
Identificatie	PKIO-certificaat en OIN van de Bewerker
Authenticatie	De Geautoriseerde Partij levert aan de Bewerker t.b.v. het samenstellen van berichten aan de BRP: • de partijcode van de Geautoriseerde Partij • met de bijbehorende Abonnementnaam
Partijen in BRP	De Geautoriseerde Partij en de Bewerker worden voor die aansluiting als partijen geregistreerd in de communicatie met de BRP.

Bijlage: relevante passages uit de Integrale versie Ontwerpaspecten mei 2014

In hoofdstuk 9 van de integrale versie van de Ontwerpaspecten (mei 2014) worden de 'Bijzondere aspecten van verstrekken' beschreven. De relevante passages in dit hoofdstuk in het kader van de bewerkersconstructies zijn hier als bijlage opgenomen.

§9.1 Inleiding
In dit hoofdstuk worden enige bijzondere aspecten die samenhangen met het verstrekken van gegevens uit de basisregistratie besproken. Eerst wordt ingegaan op de rol van bewerkers. Dit zijn organisaties die niet zelf een autorisatie hebben maar die gegevens ontvangen namens een geautoriseerde partij.

§9.2 Bewerkers
Bij het verstrekken van gegevens uit de basisregistratie, kan gebruik worden gemaakt van bewerkers. Dat betekent dat de gegevens worden verstrekt aan de geautoriseerde overheidsorganisatie of derde, maar geleverd aan een andere partij die als bewerker optreedt voor de geautoriseerde overheidsorganisatie of derde. Deze bewerker treedt dan op als ontvanger of postbus van de gegevens.[8] [9]

Omgaan met de identiteit van de geautoriseerde
In het geval dat een bewerker voor een of meerdere geautoriseerden een postbus functie vervult, moet duidelijk zijn dat de bewerker niet zelf de geautoriseerde is maar (slechts) als bewerker door een geautoriseerde is aangewezen. Dat heeft drie consequenties. In de eerste plaats dient vastgelegd te zijn bij de beheerder van de basisregistratie dat een bepaalde intermediair als bewerker voor een bepaalde geautoriseerde optreedt. Deze vastlegging dient dusdanig te zijn dat de geautoriseerde verantwoordelijk is voor hetgeen door de intermediair uit naam van de geautoriseerde wordt uitgevoerd. De geautoriseerde dient daartoe een verklaring te ondertekenen waarvan de strekking is dat de intermediair in zijn naam handelt en dat de geautoriseerde de verantwoordelijkheid voor fouten op zich neemt. Zo een verklaring moet onderdeel uitmaken van de autorisatieprocedure.

In de tweede plaats dient bij elke verstrekking vastgelegd te zijn aan welke geautoriseerde wordt verstrekt. Dat kan doordat de bewerker de identiteit van de geautoriseerde steeds in de berichten vermeld en doordat de verantwoordelijke voor de gegevensverstrekking eveneens steeds de identiteit van de geautoriseerde in de berichten vermeld. Het kenbaar maken van deze identiteit kan door een identificerend kenmerk te gebruiken zoals een uniek nummer of een unieke combinatie van gegevens zoals naam, naam gemachtigde, geboortedatum gemachtigde en dergelijke.

In de derde plaats dient er een controle uitgevoerd te worden door de centrale voorzieningen om vast te stellen of er daadwerkelijk sprake is van een autorisatie die verleend is en of daadwerkelijk de verstrekking van de gegevens door tussenkomst van de bewerker dient te geschieden. Anders gezegd: er dient authenticatie plaats te vinden van geautoriseerde en van bewerker. Voor het (geautomatiseerd) controleren van aanvragen tot gegevensverstrekking, is het wenselijk dat bij een gegevensaanvraag een referentie naar het van toepassing zijnde autorisatiebesluit wordt opgenomen of althans naar de inhoud daarvan zoals die digitaal in de BRP opgeslagen kan worden.[10]

Het kan ook zo zijn dat er gebruik wordt gemaakt van een identificerend middel waarvan het gebruik door toepassing van bepaalde technologische methoden in beginsel voorbehouden is aan de geautoriseerde. Dat kan bijvoorbeeld door gebruik te maken van een digitale handtekening De geautoriseerde doet met behulp van dit certificaat een verzoek bij zijn bewerker. De bewerker geleidt het verzoek door naar de verantwoordelijke voor de basisregistratie waarbij het certificaat ertoe dient om aan te tonen dat het verzoek van de betrokken geautoriseerde afkomstig is. Deze verdergaande

[8] De bewerker kan daarnaast ook andere rollen hebben zoals vertaler van de gegevens en als verwerker van de gegevens. Het gegeven dat een organisatie voor een geautoriseerde gegevens verwerkt, kan aanleiding zijn voor de geautoriseerde om deze organisatie ook als ontvanger van de gegevens aan te wijzen. Dat is een manier om een samenwerkingsverband tussen overheidsinstanties van de taak waarvoor wordt samengewerkt van gegevens te voorzien.

[9] Bewerkers treden op voor relatief kleine geautoriseerde organisaties (notarissen, gerechtsdeurwaarders) maar ook voor organisaties die veel van hun administratief werk hebben uitbesteed (zoals bij pensioenfondsen). Veel geautoriseerden maken gebruik van de diensten van bewerker T&T die de mogelijkheid biedt om de gegevens via verschillende interfaces te leveren.

[10] Een geautoriseerde kan op basis van het autorisatiebesluit voor meerdere doelen geautoriseerd zijn en over meerdere abonnementen beschikken. Het volstaat dan niet uitsluitend op partijID van de geautoriseerde te controleren.

vorm van authenticatie wordt niet verplicht gesteld met name omdat kleine geautoriseerde partijen daardoor relatief zwaar worden belast.

Op dit moment is de praktijk gegroeid waarin de identiteit van de geautoriseerde niet in alle gevallen kon worden achterhaald zonder gebruik te maken van informatie die bij de bewerker berust. Het gevolg daarvan is dat aan de verplichting die voortvloeit uit artikel 3.22 alleen kan worden voldaan door een beroep te doen op de bewerker. Alhoewel gesteld kan worden dat zo een beroep mogelijk is, bijvoorbeeld doordat het een onderdeel uitmaakt van de verplichtingen waaraan de bewerker is gebonden bij zijn optreden voor een geautoriseerde, is dit niet in overeenstemming met de wet. Het kan immers voorkomen dat de bewerker failliet gaat en dat geen afdoende maatregelen zijn getroffen om bijvoorbeeld vijf jaar later alsnog de benodigde gegevens aan de burger te verstrekken. Het lijkt geen optie om in die situatie alsnog een beroep te doen op de geautoriseerde teneinde te achterhalen welke gegevensverstrekkingen vijf jaar geleden door hem zijn aangevraagd en ontvangen. Door het vastleggen van de identiteit van de geautoriseerde bij elke verstrekking kan aan deze situatie een einde worden gemaakt.

Merk op dat in de gevallen waarin er geen sprake is van een bewerker, de geautoriseerde gebruik dient te maken van een digitale handtekening.

Handelen van de bewerker

Een bewerker handelt onder verantwoordelijkheid van de geautoriseerde waarvoor hij bewerker is. Het is (dus) de verantwoordelijkheid van de geautoriseerde om de relevante regelgeving, zoals met name de WBP, in acht te nemen. Wanneer bijvoorbeeld een bewerker gegevens opslaat ten behoeve van later gebruik, dan moet dat opslaan worden bezien in het licht van de werkzaamheden die onder verantwoordelijkheid van de geautoriseerde worden verricht. Voor zover er sprake is van mogelijke handelen in strijd met de regelgeving, heeft het CBP een toezichthoudende taak.

Het geval kan zich voordoen dat een bewerker voor meer dan één geautoriseerde als bewerker optreedt. In het geval dat deze bewerker in zijn rol als bewerker voor geautoriseerde A gegevens ter beschikking stelt aan zichzelf in zijn rol als bewerker voor geautoriseerde B, dan moet dit beschouwd worden als het leveren van gegevens door geautoriseerde A aan geautoriseerde B. Deze levering van gegevens vindt plaats onder de WBP en niet onder de Wet brp. Het toezicht op deze aard van gegevensverwerking berust bij het CBP.[11] [12]

[11] Merk op dat indien een geautoriseerde geen gebruik maakt van zijn autorisatiebesluit er aanleiding is om contact met deze geautoriseerde op te nemen.

[12] Dat laat onverlet dat deze handelswijze gevolgen kan hebben voor de bijdragen in de kosten van de uitvoering van de wet die geautoriseerden leveren. Op basis van gegevens over een bepaalde sector kan worden geraamd dat de typische bewerker in deze sector in de orde van grootte van 20% aan overlap in de populatie van de aangesloten organisaties heeft. Dat kan worden geconcludeerd op basis van circa 30 miljoen personen die bij een van de organisaties bekend zijn, zes miljoen personen waarmee een actieve relatie bestaat, ongeveer tien bewerkers en drie tot drieënhalf betrokken organisaties per persoon.