Pensioenfederatie
Prinses Margrietplantsoen 90
2595 BR Den Haag
Postbus 93158
2509 AD Den Haag
T +31 (0)70 76 20 220
info@pensioenfederatie.nl
www.pensioenfederatie.nl

KvK Haaglanden 52988368
IBAN: NL20TRIO0212407368
BIC: TRIONL2U

Ministerie van BZK
T.a.v. de heer M.N. Prinsen
Postbus 20011
2500 EA Den Haag

KENMERK: B/17/11139/TW
ONDERWERP: consultatie Wet GDI

DATUM: 29 maart 2017

Geachte heer Prinsen,

Hierbij stuur ik u de reactie van de Pensioenfederatie op de consultatie Wet generieke digitale infrastructuur (WGDI).

Kernboodschap van deze reactie is dat de pensioenfondsen niet verplicht willen worden tot het gebruik van de erkende authenticatiemiddelen. Meer in het algemeen kan gesteld worden dat waar het gaat om de digitale diensten van de overheid, of het nu gaat om de Berichtenbox, het gebruik van de BRP of DigiD er een grote discrepantie is tussen de mogelijkheid om mee te bepalen en de dwang tot meebetalen.

We willen graag met de overheid in gesprek over de bredere context. Voor de Pensioenfederatie is het niet vanzelfsprekend dat de pensioenfondsen gebruikmaken van de digitale diensten die de overheid aanbiedt. Natuurlijk zijn daaraan, ook voor de deelnemers, vele voordelen verbonden. Echter, het gebrek aan vrijheid, inspraak en de alsmaar stijgende rekeningen zijn een fors nadeel voor de deelnemer. Deze nadelen kunnen een heroverweging van de koers die de pensioenfondsen nu varen, gericht op aansluiting bij de digitale overheidsdiensten, noodzakelijk maken.

Wij zijn van harte bereid onze reactie mondeling toe te lichten. Indien u dit op prijs stelt, verzoek ik u contact op te nemen met Julia Adam, adam@pensioenfederatie.nl.

Met vriendelijke groet,

Gerard Riemen
Algemeen directeur

**Algemene opmerkingen naar aanleiding van de consultatie**

Waar pensioenuitvoerders aanvankelijk ieder voor zich een eigen inlogmechanisme hadden, deed op enig moment DigiD zijn intrede. Tot ieders tevredenheid, zolang het een veilige inlogmethode is. Het wetsvoorstel maakt een scala aan inlogmechanismen mogelijk. Dat lijkt zijn doel voorbij te schieten, waar het veilig en betrouwbaar maken van DigiD voldoende zou moeten zijn.

*We onderschrijven het belang van digitale veiligheid en gebruikersgemak*

De pensioensector onderschrijft het belang dat het kabinet met dit wetsvoorstel uitdraagt ten aanzien van privacy en veiligheid van gegevens van deelnemers. Die gegevens moeten kunnen worden ontsloten via platforms die de deelnemer informeren of adviseren bij pensioenkeuzes. Eenvoud en gebruikersgemak voor deelnemers staan daarbij voor pensioenfondsen voorop. Het wetvoorstel verbetert de digitale dienstverlening. De multimiddelenaanpak die uitgangspunt is van het wetsvoorstel, maakt het voor meer deelnemers mogelijk om in te loggen op de Mijn-omgeving van de pensioenfondsen of makkelijker om te navigeren naar mijnpensioenoverzicht.nl.

*Maar pensioenuitvoerders hebben andere kenmerken en een andere dynamiek dan overheidsinstanties*

De dienstverlening door de pensioensector heeft andere kenmerken en een andere dynamiek dan veel overheidsinstanties en kent daarmee vaak andere behoeftes of urgenties op het gebied van authenticatie en identificatie. Het aanvullende 2e pijlerpensioen is een onderdeel van het totale pensioeninkomen. We verwachten dat de behoefte aan een totaal financieel advies zal toenemen. Deelnemers zullen verder willen kijken dan alleen de 2e pijler en hun pensioengegevens steeds meer willen combineren met andere gegevens over hun financiële situatie. Dat maakt de situatie van pensioenuitvoerders anders dan voor instanties als de Belastingdienst of het Kadaster. DigiD is een middel dat onmiskenbaar z'n voordelen heeft voor deelnemers en pensioenfondsen (voor de meeste burgers is dit een bekend inlogmiddel). Maar het kent zeker ook zijn beperkingen (werkt alleen binnen Nederland en alleen in de 2e pijler en bij overheidsinstanties). Een ander voorbeeld is het Pensioenregister. Daarin ziet de deelnemer zijn AOW- en zijn 2e pijlerpensioen. Maar zijn inkomensvoorzieningen uit de 3e pijler ontbreken.

Zouden die laatste voorzieningen wel deel uitmaken van het Pensioenregister, dan zou DigiD weer niet gebruikt kunnen worden.

*Het wetsvoorstel heeft nadelen voor de pensioensector en haar deelnemers*
De deelnemer staat centraal bij de pensioenfondsen. Dat betekent dat fondsen beschikbare middelen willen beoordelen op aspecten als gebruikersgemak en acceptatiegraad van de deelnemer. Enerzijds kan dit fondsen ertoe bewegen om een zo breed mogelijk aanbod van actuele middelen te doen aan hun deelnemers. Het wetsvoorstel kan fondsen beperken in hun mogelijkheden daarin. Met het wetsvoorstel wordt de pensioensector immers gehouden aan het gebruik van erkende publieke en private authenticatiemiddelen. Dat zou in een extreme situatie tot gevolg kunnen hebben dat er straks bijvoorbeeld vier middelen beschikbaar zijn, die de deelnemer niet ziet zitten. Anderzijds kan het fondsen ertoe brengen de keuzes qua middelen te willen beperken ter voorkoming van keuzestress bij deelnemers. Ook dat kan in het belang van deelnemers zijn.

We zien daarom als nadeel dat we als pensioensector geen invloed hebben op de voor erkenning gekozen middelen en de eisen waaraan die middelen moeten voldoen. Evenmin hebben we invloed op de goedkeurings- en implementatietermijnen van nieuwe middelen. De verdere doorontwikkeling van bestaande overheidsauthenticatiemiddelen is daarnaast afhankelijk van de prioritering en verandersnelheid van de overheid. Ook daarop heeft de pensioensector geen invloed.

Bovendien hebben we, zeker bij de publieke middelen, de kosten niet zelf in de hand. In de toelichting bij het wetsvoorstel is te lezen dat het gebruik ervan doorbelast kan worden aan de overheidsinstanties en de aangewezen organisaties. Zie ook de nog lopende discussie over de financiering van de Berichtenbox. De structurele kosten van de Berichtenbox blijken vele malen hoger te zijn dan de eenmalige kosten waarvan de overheid bij aanvang van de Berichtenbox was uitgegaan. De consequentie is dat kosten onvoorspelbaar zijn.

Verder wijzen we op de druk die op de fondsen ligt, om de uitvoeringskosten naar beneden te brengen.

Een onvoorspelbaar onderdeel van die kosten is dan onacceptabel. In het belang van het fonds en diens deelnemers zou daarom de keuze voor een goedkoper middel open moeten staan.

*Maar waarom is er überhaupt een wettelijke acceptatieplicht?*
Los van de nadelen die het wetsvoorstel voor de pensioensector heeft, is de vraag überhaupt wat de noodzaak is om pensioenuitvoerders te verplichten tot gebruik van de erkende authenticatiemiddelen?
Om fondsen alleen middelen te laten gebruiken die voldoen aan bepaalde eisen, volstaat de verplichting tot certificering. Dat authenticatiemiddelen moeten voldoen aan bepaalde eisen, daarvan zijn wij alleen maar voorstander. Een erkenning vanuit overheidswege biedt het pensioenfonds en zijn deelnemers meer comfort bij de keuze voor dat middel. De erkenning is een vorm van certificering, een keurmerk. En dat is goed.

Maar een wettelijke acceptatieplicht om te voorkomen dat burgers en ondernemers voor elke publieke dienstverlener een ander middel zouden moeten gebruiken, vinden we te vergaand. Juist pensioenuitvoerders hebben er belang bij hun deelnemers middelen aan te bieden die zij kennen en ook voor andere toepassingen gebruiken. Pensioenuitvoerders zouden anders hun eigen digitale diensten ontoegankelijk maken. Er is dus geen wet nodig om pensioenuitvoerders algemeen gebruikte middelen te laten hanteren.

Ook beperkt de verplichtstelling de (toekomstige) mogelijkheden voor pensioenuitvoerders. Uit de toelichting blijkt dat het de bedoeling is om ruimte open te laten voor technologische ontwikkelingen. Maar ontwikkelingen op dit terrein gaan hard. Onbedoeld kunnen wet- en regelgeving toch onnodige beperkingen opleggen. Voorkomen moet worden dat met de nieuwe wet pensioenuitvoerders in een ‘overheidsnet’ gevangen zitten en geen gebruik kunnen maken van mooie, innovatieve oplossingen uit de markt.

## Uitvoerbaarheid van het voorstel

In de vorige paragraaf hebben we onze bezwaren tegen de wettelijke acceptatieplicht uiteen gezet. Mocht deze verplichting gehandhaafd blijven, dan plaatsen we hieronder een aantal kanttekeningen bij de uitvoerbaarheid van het wetsvoorstel zoals dat nu voorligt. Voor de volledigheid, we zijn tegen het introduceren van de wettelijke plicht om erkende middelen te accepteren.

Maar we zijn wél voorstander van de ontwikkeling van dergelijke middelen en het gebruik ervan. Onderstaande punten over de uitvoerbaarheid van het wetsvoorstel geven we daarom ook mee voor de situatie dat de wettelijke acceptatieplicht komt te vervallen in het definitieve wetsvoorstel. In dat geval is het aan de fondsen om ieder voor zich een afweging te maken tussen middelen en kosten.

*De grote lijn is duidelijk en uitvoerbaar*

Het wetsvoorstel heeft impact op de pensioensector. Pensioenuitvoerders moeten een aantal voorzieningen inrichten en inpassen in de uitvoering. Zo moeten diverse inlogsystemen voor deelnemers, werkgevers, salarisadministrateurs en gegevensleveranciers aangepast worden, moet de huidige koppeling met DigiD ontmanteld worden, moet er een functionaliteit voor machtigingen in de Mijn-omgevingen ingericht worden, moet er integratie met ontsluitende diensten via koppelvlakken plaatsvinden en moet de informatie ten behoeve van de onafhankelijke audits ingeregeld worden. Naast de technische kant zullen deelnemers, werkgevers, gegevensleveranciers en salarisadministrateurs geïnformeerd en ondersteund moeten worden.
Dit alles brengt uiteraard ook kosten met zich mee (investeringskosten, licentiekosten, ontwikkelkosten).
Beheers- en onderhoudskosten zijn er als er wijzigingen geïmplementeerd moeten worden.

*Maar veel details zijn nog onduidelijk*

Veel details van het automatiseringsvraagstuk, die nodig zijn voor de uiteindelijke inrichting van systemen, ontbreken nog. Zo is nog onduidelijk hoe het koppelvlak c.q. de koppelvlakken eruit zien. Ook de vraag elke diensten een ontsluitende organisatie biedt ten behoeve van integratie (technisch, procesmatig) is nog onduidelijk.

*Aansluiting van alle pensioenuitvoerders, ieder voor zich, is niet kostenefficiënt*

De ontsluitende dienst verzorgt de aansluiting van de publieke dienstverleners op de erkende middelen (vergelijkbaar met iDeal).

Alle pensioenuitvoerders en andere aangewezen organisaties c.q. alle bestuursorganen dienen, ieder voor zich, een koppelvlak (mogelijk een koppelvlak per middel) te ontwikkelen naar een ontsluitende dienst. Die inspanning verschilt per pensioenuitvoerder.
Voor de pensioensector als totaal zal het verplichte gebruik tot aanzienlijke initiële en onderhoudskosten leiden. We adviseren dan ook om te onderzoeken of en op welke manier de overheid de aansluiting van meerdere organisaties/sectoren kan faciliteren, zodat er schaalvoordeel behaald kan worden. Dat zou wellicht een implementatiedienst van private partijen of een uniform landelijk koppelvlak kunnen zijn.

**Handhaafbaarheid**

*Toezichthouders*

Naleving van de wet wordt voorzien door het aanwijzen van toezichthouders. Ook voor de aangewezen organisaties. Men wil dit zoveel mogelijk binnen de bestaande toezichtstructuren inregelen. De minister wijst toezichthouders aan. Om de toezichtlast voor pensioenfondsen niet te breed te laten zijn, zou het voor de hand liggen het toezicht bij DNB of de AP te leggen. Wel moeten de betreffende medewerkers van die toezichthoudende organen voldoende kennis hebben over deze materie.

*Audit*

Daarnaast moet jaarlijks door een onafhankelijke auditor een verklaring aan BZK worden aangeboden (toets of de elektronische dienstverlening daadwerkelijk aan de eisen voldoet). Maar daarbij wordt aangesloten op de huidige systematiek die wordt gehanteerd bij de aansluiting op DigiD (vraag: zou dus voor de fondsen geen meerwerk moeten zijn?). Volgens de consultatieversie wordt ook verwacht dat de kosten van deze audit in de orde van grootte van de huidige DigiD-assessments liggen. Waarop is deze veronderstelling gebaseerd?

**Onderwerpen waar nog onduidelijkheid over bestaat**

We noemen er een aantal, zonder uitputtend te zijn.

*Uitvoeringsregels*

In de nog op te stellen uitvoeringsregelgeving worden veel elementen uitgewerkt. Dat betekent dat het wetsvoorstel nog veel onduidelijkheden met zich meebrengt.

Het is noodzaak om zo snel mogelijk inzicht te krijgen in deze nadere regels. Zo zal de uitvoeringsregelgeving ook bewaartermijnen stellen t.a.v. de persoonsgegevens die nodig zijn om toegang te geven/krijgen tot elektronische diensten. Dit zijn aspecten die in een vroeg stadium al duidelijk moeten zijn.
Ook is een vraag of voor de publieke en private middelen dezelfde criteria gaan gelden? En hoelang is de procedure voor erkenning?

*Onderscheid bestuursorganen – aangewezen organisaties*
Het wetsvoorstel is van toepassing op bestuursorganen (kort gezegd: overheidsinstanties) en aangewezen organisaties (kort gezegd: BSN-organisaties). In het wetsvoorstel/de toelichting lijken beide begrippen door elkaar te lopen. Zie bv. pag. 26 van de toelichting: het wetsvoorstel stelt eisen aan de informatiebeveiliging. Ook voor aansluitende systemen moeten passende maatregelen genomen worden om aantasting of inbreuk te voorkomen. Daarbij wordt aangesloten bij de rijksbrede relevante normen en verplichte open standaarden. Maar de verplichting om aangewezen open standaarden te gebruiken, geldt in dit wetsvoorstel alleen voor overheidsinstanties. Onduidelijk is of de verplichting via deze weg ook voor aangewezen organisaties geldt?

*Aansprakelijkheid*
Openstaand punt is ook de aansprakelijkheid. Als er iets mis blijkt te zijn met een verplicht middel, dan kunnen fondsen niet aansprakelijk gehouden worden voor de schade. We hebben immers geen keuze in wel of niet dat middel accepteren. Ervan uitgaande dat de fondsen volgens de jaarlijkse audit voldoen aan de gestelde eisen dan wel de fondsen anderszins geen verwijt valt te maken.

*Misbruik gegevens*
Bij een hoog beveiligingsniveau is een van de mogelijkheden om identificatie plaats te laten vinden via een ID kaart met daarin opgenomen een chip met de benodigde gegevens.
Hoe wordt voorkomen dat de gegevens op de ID gestolen of misbruikt kunnen worden (in de bankwereld is skimming een vergelijkbaar probleem)?

*Algemeen gebruik authenticatiemiddelen*
Het wetsvoorstel geldt niet voor andere financiële sectoren dan 2e pijler pensioen. De ontwikkeling naar een bredere financiële dienstverlener, maar ook nu vanuit het perspectief van de deelnemer die aan financiële planning wil doen, zou de mogelijkheid om gegevens te ontsluiten breder moeten zijn dan in dit voorstel.

Uit de toelichting is af te leiden dat publieke authenticatiemiddelen, zoals DigiD, niet gebruikt kunnen worden voor gebruik buiten het publieke domein (zie MvT, o.a. pag. 15). Dat is vanuit gebruikersgemak zeer onwenselijk. Een deelnemer wil het eenmaal gekozen middel het liefst gebruiken voor al zijn financiële planning, en liefst ook via de 'single sign on'- methode. Zodat hij vanuit het Pensioenregister direct door kan naar zijn hypotheekgegevens. Overigens wordt ook nu al binnen de 2e pijler gebruikgemaakt van c.q. gewerkt aan single sign on methodes, bv. via Logius. Migratie van DigiD naar een hoger beveiligingsniveau zou er niet toe moeten leiden dat single sign on onmogelijk wordt gemaakt.