Position Paper

Verordening digitale operationele weerbaarheid (DORA)

Op 24 september 2020 heeft de Europese Commissie een voorstel gepubliceerd voor de Verordening digitale operationele weerbaarheid (DORA). Met deze verordening wil de Europese Commissie de minimumvereisten voor digitale weerbaarheid voor financiële instellingen harmoniseren en regels stellen om de digitale risico's bij uitbestedingspartijen beter te beheersen. Door middel van een verordening, die geen implementatie in nationale wetgeving behoeft, beoogt het voorstel de vereisten voor financiële instellingen uit verschillende sectoren en lidstaten gelijk te trekken. Ook pensioenfondsen moeten in het voorstel van de Europese Commissie voldoen aan de vereisten. Tijdens een consultatie ter voorbereiding van het wetgevende voorstel werden pensioenfondsen niet genoemd, waardoor het leek dat het voorstel geen directe betrekking zou hebben op de sector. De Pensioenfederatie voelt zich dan ook geroepen om te reageren op het voorstel van de Europese Commissie.

De Pensioenfederatie herkent zich in de geest van de verordening. De vereisten zijn afgeleid van gangbare internationale standaarden en aanbevelingen. Samen met De Nederlandsche Bank heeft de pensioensector de afgelopen jaren grote stappen gezet om aan deze standaarden te voldoen. De impact van de verordening op de informatiebeveiliging lijkt dan ook gering, gegeven het relatief hoge niveau van informatiebeveiliging van de Nederlandse pensioensector.

Tegelijkertijd maakt de Pensioenfederatie zich zorgen over de mate van detail waarin regelgeving voor de financiële sector in het algemeen, en de DORA-verordening in het bijzonder, wordt opgesteld. Een verordening geeft immers minder flexibiliteit dan een toezichtskader, zowel aan toezichthouder als aan de pensioensector. De Pensioenfederatie roept de nationale toezichthouders op om bij de implementatie de constructieve dialoog die de er tussen de sector en toezichthouders tot stand is gekomen, voort te zetten onder het nieuwe DORA-kader. Alhoewel de sector zich in het algemeen kan vinden in de inhoud van de voorgestelde regels, is het van cruciaal belang dat proportionaliteit een leidend principe blijft bij het toezicht, zodat er samen overlegd kan blijven worden over de maatregelen die het meest passend zijn voor de specifieke situatie waarin Nederlandse pensioenfondsen zich bevinden.

De Pensioenfederatie wil de Europese Commissie daarnaast oproepen om ook zelf in actie te komen om de digitale weerbaarheid van de Europese financiële markten te verhogen. DORA verhoogt de rapportage- en toezichtlasten van de Nederlandse pensioensector. Hier staan vooralsnog geen voordelen voor de Nederlandse pensioendeelnemers tegenover. Zo zou de

Pensioenfederatie graag zien dat ook pensioenfondsen kunnen profiteren van de verzamelde ICT-incident informatie. Tevens ziet de Pensioenfederatie graag dat de Europese toezichthouders de IT-risico's bij grote leveranciers gaan identificeren en beheersen.

Hieronder volgen meer in detail de aandachtspunten van de Pensioenfederatie bij de verschillende hoofdstukken van de verordening.

Hoofdstuk II ICT Risico Management

In hoofdstuk II worden verschillende maatregelen opgesomd die financiële instellingen moeten treffen om de digitale weerbaarheid op niveau te houden. Deze maatregelen zijn afgeleid uit internationale standaarden en daarmee niet nieuw voor de Nederlandse pensioensector. Het voorstel gaat niet in op de vraag in hoeverre de uitvoering van deze maatregelen kan worden overgelaten aan uitbestedingspartijen. Voor Nederlandse pensioenfondsen en hun uitbestedingspartijen is het verhelderen van deze onduidelijkheid van cruciaal belang.[1] De meeste Nederlandse pensioenfondsen hebben hun belangrijkste ICT-activiteiten namelijk uitbesteed aan professionele partijen, zoals pensioenuitvoeringsorganisaties. De meeste Nederlandse pensioenfondsen beheren dan ook niet de systemen die verantwoordelijk zijn voor het verwerken van persoonsgegevens van deelnemers, het betalen van pensioenuitkeringen of het dagelijkse beheer van de beleggingen. Nederlandse pensioenfondsen beheersen het ICT-risico daarom ook via hun uitbestedingsrelatie, alhoewel het pensioenfonds zelf verantwoordelijk blijft voor het risicomanagement. Het door het pensioenfonds zelf uitvoeren van alle maatregelen die opgesomd zijn in hoofdstuk II, zou een enorme verhoging van kosten met zich meebrengen, zonder dat de digitale weerbaarheid van de Nederlandse pensioensector daarmee vooruitgaat.

Momenteel is het toezicht op de beheersing van cyberrisico's bij pensioenfondsen gebaseerd op de bepalingen uit IORP II. Ook die zijn enkel van toepassing op pensioenfondsen zelf, maar in de toezichtspraktijk worden uitbestedingspartijen nauw betrokken. Via de bepalingen in IORP II heeft DNB op deze wijze een 'indirect' mandaat om goed toe te zien op de risicobeheersing bij pensioenuitvoeringsorganisaties. Dit lijkt in algemene zin goed te werken. De Pensioenfederatie roept op om ervoor te zorgen dat er in de DORA-verordening geen bepalingen worden opgenomen die dit 'indirecte' toezicht ondermijnen door het onmogelijk maken van het uitbesteden van het ICT-risicomanagement.

Hoofdstuk III ICT incidenten

Verschillende Nederlandse financiële instellingen vallen onder de reikwijdte van de NIB-richtlijn (c.q. Wet beveiliging netwerk- en informatiesystemen). Zij rapporteren ICT-

[1] Dit betreft niet alleen het verduidelijken van de bepalingen in hoofdstuk II, maar ook de precieze definitie van ICT-toeleverancier (ICT third-party service providers) en de samenhang.

incidenten aan De Nederlandsche Bank en maken aanspraak op bijstand, informatie en adviezen vanuit het Nationaal Cybersecurity Centrum (NCSC). Voor Nederlandse pensioenfondsen en uitvoeringsorganisaties gelden deze vereisten en aanspraken op dit moment (nog) niet.

De verordening introduceert de verplichting voor alle financiële instellingen, inclusief pensioenfondsen, om ICT-incidenten binnen enkele uren te melden bij de nationale toezichthouder. Dit is een nieuwe rapportageverplichting voor financiële instellingen die niet onder de NIB-richtlijn vallen (zoals pensioenfondsen), al zal de precieze impact afhankelijk zijn van de materialiteitsdrempel die wordt gehanteerd voor het melden van incidenten.

Dit neemt niet weg dat deze rapportageverplichting op twee punten onevenwichtig is. In de eerste plaats is deze verplichting onevenwichtig omdat dezelfde rapportageverplichting geldt voor "cruciale" financiële instellingen die onder de NIB-richtlijn vallen (en daarmee aanspraak kunnen maken op ondersteuning vanuit het NCSC) en financiële instellingen die niet als cruciaal worden aangemerkt. De verplichting is in de tweede plaats onevenwichtig omdat tegenover de korte notificatie termijnen in het convenant (vooralsnog) geen verplichting voor de toezichthouders staat om snel opvolging te geven. De Pensioenfederatie pleit er dan ook tot die tijd voor dat financiële instellingen die niet onder de NIB-richtlijn vallen niet hoeven te rapporteren. Hiermee wordt cruciale capaciteit vrijgespeeld om digitale aanvallen te kunnen weerstaan.

Hoofdstuk IV Digitale operationele weerbaarheidstest
De Pensioenfederatie verwelkomt het feit dat de Nederlandse TIBER-test in Europese wetgeving wordt verankerd. Het initiatief van De Nederlandsche Bank heeft een waardevolle bijdrage geleverd aan de digitale weerbaarheid van Nederlandse financiële instellingen. De Pensioenfederatie pleit er hierbij wel voor dat ook ICT-toeleveranciers (ICT third-party service providers) worden verplicht om mee te doen in dergelijke weerbaarheidstesten. Hiermee wordt tegemoetgekomen aan een beperking van de Nederlandse testen en een betere test op het niveau van de Europese Unie geïntroduceerd.

Hoofdstuk V ICT-third party risk
De Pensioenfederatie is ook blij dat ICT-toeleveranciers onder de reikwijdte van de verordening worden gebracht. De positie van ook de Nederlandse pensioensector tegenover met name Amerikaanse aanbieders van clouddiensten wordt hiermee versterkt. Tegelijkertijd vraagt de introductie van deze nieuwe verplichtingen wel een zekere mate van proportionaliteit tussen de activiteiten van de toezichthouders en financiële instellingen. Pensioenfondsen kunnen effectief de rechten tot toegang, inspectie en audit uitoefenen bij bijvoorbeeld nationale telecomaanbieders en kleine tot middelgrote ICT-toeleveranciers. Het uitoefenen van deze rechten is echter weinig effectief bij de grote Amerikaanse aanbieders

van clouddiensten. Dergelijke inspecties en audits kunnen het beste centraal worden uitgevoerd door de Europese toezichthouders. Samen maken we daarmee een sterke Europese Unie.