Fiche 4: Verordening digitale operationele weerbaarheid (DORA)

1. Algemene gegevens

a) Titel voorstel

Verordening van het Europese Parlement en de Raad betreffende digitale operationele weerbaarheid voor de financiële sector en amendering van verordeningen (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 en (EU) No 909/2014.

b) Datum ontvangst Commissiedocument

24 september 2020

c) Nr. Commissiedocument

COM(2020) 595

d) EUR-lex

https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1601475955102&uri=CELEX:52020PC0595

e) Nr. impact assessment Commissie en Opinie Raad voor Regelgevingstoetsing

SWD(2020) 198

f) Behandelingstraject Raad

Raad Economische en Financiële Zaken

g) Eerstverantwoordelijk ministerie

Ministerie van Financiën

h) Rechtsbasis

Artikel 114 van het Verdrag betreffende de werking van de Europese Unie (VWEU).

i) Besluitvormingsprocedure Raad

Gekwalificeerde meerderheid

j) Rol Europees Parlement

Medebeslissing

2. Essentie voorstel

a) Inhoud voorstel

Na de financiële crisis zijn er veel wijzigingen in het regelgevend kader voor de financiële sector aangebracht, voornamelijk omtrent de prudentiële risico's van financiële dienstverlening. Een bredere ontwikkeling van digitalisering heeft tot gevolg dat bedrijven, overheden en organisaties steeds meer cyberrisico's lopen, zo ook de financiële sector. In de afgelopen jaren zijn digitale

ketens groter geworden, is de connectiviteit tussen instellingen en derde partijen toegenomen en is het potentiële aanvalsoppervlak van instellingen vergroot. ICT-verstoringen bij financiële instellingen kunnen tot grote problemen leiden, en cyberrisico's hebben daarom ook steeds meer risico's voor de financiële stabiliteit.

Hoewel er reeds Unieregels bestaan die zien op operationele en cyberrisico's, gelden deze maar voor een klein aantal typen dienstenaanbieders, zoals kredietinstellingen en betaalinstellingen. Voor overige financiële dienstverleners hebben sommige lidstaten zelf regelgevende kaders opgesteld, maar bestaan er in veel gevallen alleen algemene normen of zelfs helemaal geen regels. Het ICT-governance kader voor financiële instellingen is daardoor zeer versnipperd. Dit maakt effectief toezicht houden moeilijk en leidt tot inconsistenties in wet- en regelgeving tussen lidstaten, en onnodige kosten voor de sector. Om bovenstaande redenen heeft de Commissie een voorstel gedaan om in de Unie te komen tot een eenvormig wetgevend kader ten aanzien van digitale weerbaarheid in de gehele financiële sector, als onderdeel van het *Digital Finance Package.*

De Commissie heeft drie hoofddoelen voor ogen gehouden bij het opstellen van Verordening digitale operationele weerbaarheid (Digital Operational Resilience Act - DORA). Enerzijds moet het de reeds bestaande, maar versnipperde en soms weinig specifieke Unieregels ten aanzien van cyberweerbaarheid van de financiële sector combineren en harmoniseren in een overkoepelende verordening, in een minder algemene vorm. Anderzijds creëert DORA een kader voor financiële instellingen waarvoor nog geen specifieke cyberweerbaarheidregels bestonden. Tenslotte bevat het voorstel regels om de risico's van uitbesteding door de financiële sector aan kritieke digitale derde dienstverleners beter te mitigeren en om de versnippering van de regels daaromtrent tegen te gaan. DORA laat reeds bestaande generieke wetgeving ter versterking van de weerbaarheid in stand.[1]

De voorgestelde verordening bestaat uit vijf onderdelen. Allereerst bevat het een algemeen kader waarbinnen financiële instellingen verplicht worden om maatregelen te nemen die het risico op ICT-incidenten verlaagt. Hieronder vallen verplichtingen tot het opzetten en onderhouden van weerbare ICT-systemen, het nemen van beschermings- en preventiemaatregelen en het maken van continuïteitsplannen. Vervolgens worden financiële instellingen verplicht om grote ICT-incidenten te melden, en hiervoor systemen op te zetten waarmee incidenten gemonitord, vastgelegd en geclassificeerd worden. Financiële instellingen dienen daarnaast periodiek de cyberweerbaarheid te testen op paraatheid en eventuele zwaktes en tekortkomingen. Alle financiële instellingen zullen hierbij jaarlijks hun ICT-systemen dienen te testen op een bepaald basisniveau, waarbij significante instellingen, die worden aangewezen door bevoegde toezichthouders, ook minimaal eens per drie jaar geavanceerde ethische hacktesten op basis van actuele dreigingsinformatie zullen ondergaan, zogenaamd '*Threat Led Penetration Testing'* (TLPT).

[1] Bijv. het horizontale kader voor cybersecurity (NIB-Richtlijn) en de European Critical Infrastructure Directive, Ook sluit het aan bij strategische initiatieven zoals de Europese datastrategie en de veiligheidsuniestrategie.

Voorts worden er bepalingen voorgesteld ten aanzien van derde partijen die ICT-diensten aanbieden aan financiële instellingen. Financiële instellingen die gebruik maken van de diensten van bepaalde derde partijen (bijv. clouddienstverleners) zullen bijvoorbeeld het functioneren van deze diensten, en de eventuele bijkomende risico's, moeten blijven monitoren. Om deze monitoring effectief uit te kunnen oefenen worden bepaalde aspecten van de dienstverlening en de relatie tussen dienstverlener en financiële instelling geharmoniseerd en gestandaardiseerd, zoals verplichte contractuele afspraken over bijvoorbeeld de locaties waar persoonlijke data wordt verwerkt en eventuele exit-strategieën als de financiële instelling wil overstappen van aanbieder. Naast gestandaardiseerde contractclausules zullen ook vrijwillige clausules worden ontwikkeld, specifiek voor clouddienstverleners. Kritieke derde dienstverleners worden onderworpen aan een toezichtkader op Unieniveau. Dienstverleners worden kritiek geacht op basis van (een combinatie van) de aard, omvang, en het belang van hun diensten, klanten, en marktaandeel, alsmede mate waarin hun dienstverlening te substitueren is en de grensoverschreidendheid daarvan. De aangewezen toezichthouders krijgen mogelijkheden om onder andere audits uit te voeren, en niet-bindende aanbevelingen te doen aan de dienstverlener. Tenslotte bevat de verordening voorstellen waarbij financiële entiteiten wordt toegestaan om onderling informatie over cyberbedreigingen te delen.

Zoals eerder genoemd is één van de doelen van deze Verordening het harmoniseren van bestaande regels. Dit wordt grotendeels gedaan via de zogenaamde *amending directive*, waarmee geregeld wordt dat de bestaande Unieregels omtrent de beheersing van ICT-risico's aansluiting vinden bij de bepalingen in DORA.[2]

b) Impact assessment Commissie

De Commissie heeft meerdere opties onderzocht bij het opstellen van de verordening. Hierbij is gekeken naar een "status quo"-optie, waarbij de operationele weerbaarheid in de financiële sector gedeeltelijk door sectorale wetgeving, en gedeeltelijk door generieke wetgeving (zoals de richtlijn beveiliging netwerk- en informatiesystemen - NIB-richtlijn) wordt gereguleerd, aangevuld door nationale regimes. De eerste wetgevende optie betrof het verhogen van eisen aan kapitaalbuffers, om zo ervoor te zorgen dat eventuele verliezen door operationele incidenten kunnen worden opgevangen. De tweede wetgevende optie betrof een verordening, in combinatie met een toezichtraamwerk voor derde dienstverleners zoals deze uiteindelijk is voorgesteld. De derde optie betrof tenslotte een verordening zoals onderhavig voorstel, in combinatie met een nieuw op te zetten Unie-autoriteit die direct toezicht houdt op kritieke derde dienstverleners.

De status quo optie viel af omdat deze geen verandering brengt aan de huidige situatie waar regulering versnipperd is en in sommige gevallen incompleet. Optie 1 viel af omdat deze optie niet direct leidt tot verbeteringen aan operationele weerbaarheid, maar alleen aan de financiële situatie van een instelling. Hiermee zou er grote kans zijn dat de beleidsdoelstelling niet behaald zou

[2] COM (2020)596, Richtlijn van het Europese Parlement en de Raad betreffende het amenderen van richtlijnen 006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 en EU/2016/2341. Deze richtlijn bevat technische aanpassingen. Deze aanpassingen worden door Nederland gesteund.

worden. Optie 3 viel af omdat het opzetten van een specifieke Unie-autoriteit op dit moment een te vergaande en weinig efficiënte oplossing zou zijn. De kosten en moeite voor het opzetten van een nieuwe Unie-autoriteit zou op dit moment niet opwegen tegen de baten.

3. Nederlandse positie ten aanzien van het voorstel

a) Essentie Nederlands beleid op dit terrein

Het kabinet hecht grote waarde aan een sterke digitale weerbaarheid van de overheid, het bedrijfsleven en de maatschappij in het algemeen, en de financiële sector in het bijzonder. Het weerbaar maken van Nederland tegen digitale dreigingen wordt door het kabinet op geïntegreerde wijze geadresseerd met de Nederlandse Cyber Security Agenda.[3] Gezien het inherent grensoverschrijdende karakter van cyberbeveiliging en cyberdreiging staan Europese en internationale samenwerking in de Nederlandse aanpak op dit terrein centraal. Ook ten aanzien van de financiële sector in het bijzonder hecht het kabinet grote waarde aan een hoge mate van cyberweerbaarheid. Zo heeft Nederland voor een aantal financiële diensten op nationaal niveau operationele eisen opgelegd, zoals via de Regeling oversight goede werking betalingsverkeer. Daarnaast hechten de financiële toezichthouders, de Autoriteit Financiële Markten (AFM) en De Nederlandsche Bank (DNB), grote waarde aan digitale weerbaarheid. Zowel AFM[4] als DNB[5] hebben in hun toezichtstrategieën aangegeven de komende jaren prioriteiten te geven aan operationele en digitale dreigingen. De toezichthouders beschikken daarvoor ook over de benodigde expertise. Zo is het Nederlandse TIBER-model voor *Threat Level Penetration Testing* (TLPT) op EU-niveau door de ECB overgenomen als de standaard voor ethische hacktests op basis van actuele dreigingsinformatie bij kritische financiële dienstverleners in de gehele Unie.

Ook ten aanzien van bepaalde categorieën van de derde partij ICT-dienstverleners is reeds bestaande regelgeving. Op grond van de NIB-richtlijn geldt er voor zogeheten digitale dienstverleners al een zorgplicht; tot de digitale dienstverleners behoren ook clouddienstverleners. Dat betekent dat zij passende en evenredige technische en organisatorische maatregelen moeten nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen die zijn gebruiken om hun clouddiensten aan te bieden te beheersen. In de uitvoeringsverordening zijn de beveiligingseisen die deze aanbieders moeten treffen nader uitgewerkt. Ook hebben zij een meldplicht van incidenten. Op zowel de meldplicht als zorgplicht houdt Agentschap Telecom toezicht.

Tenslotte concludeert het kabinet dat de toenemende digitalisering van financiële dienstverlening ertoe leidt dat digitale en operationele dreigingen een steeds grotere risicofactor wordt voor financiële stabiliteit en het vertrouwen in het financiële systeem. Hierbij geldt ook dat de digitale ketens van financiële instellingen vaker tussenschakels bevatten. Steeds vaker worden kritieke bedrijfsprocessen, met name op ICT-gebied, uitbesteed aan derde partijen die toegang hebben tot

[3] Kamerbrief van 20 april 2018, Tweede Kamer, Vergaderjaar 2017-2018, 26643, nr. 536 25 juni 2020, Tweede Kamer, Vergaderjaar 2019-2020, nr. 2020Z12222

[4] Zie: https://www.afm.nl/nl-nl/verslaglegging/strategie-2020-2022

[5] https://www.dnb.nl/toezichtprofessioneel/visie-op-toezicht/index.jsp

of behoren tot hun (kern)infrastructuur. Hoewel dit geen slechte ontwikkeling is, aangezien het kan leiden tot innovatievere en efficiëntere dienstverlening, betekent dit vanuit operationeel oogpunt dat er meer schakels in een keten ontstaan waarbij operationele problemen kunnen ontstaan. De financiële instelling kan bijvoorbeeld via de derde partij zelf het doel van een cyberaanval zijn, maar evengoed slachtoffer worden van een succesvolle cyberaanval op de dienstverlener. Hierbij gaat het vaak om dienstverleners die niet vergunningplichtig zijn (op basis van financiële regelgeving), waardoor de financiële toezichthouders geen, of beperkt, mandaat hebben om enige vorm van toezicht op deze partijen uit te oefenen. Voorbeeld hiervan zijn partijen die clouddiensten aanbieden, waarin financiële instellingen hun ICT-diensten hebben ondergebracht.

b) Beoordeling + inzet ten aanzien van dit voorstel

Het kabinet verwelkomt het voorstel van de Commissie voor een verordening voor digitale en operationele weerbaarheid en ziet het als een belangrijke stap in de harmonisatie van operationaliteitseisen voor de financiële sector. Ook het kabinet signaleert dat er op Europees niveau een versnipperd kader bestaat voor cyberweerbaarheid van de financiële sector. De aanpak van cyberdreigingen wordt verschillend opgepakt door lidstaten en hun toezichthouders, wat leidt tot inefficiëntie en een ongelijk speelveld, doordat instellingen in verschillende lidstaten zich aan meer of juist minder strenge eisen hoeven te houden. Ook acht het kabinet het van belang dat verschillende Europese wetgeving gericht op het versterken van de digitale weerbaarheid, zowel generieke als sectorale, zoveel mogelijk op elkaar aansluiten en gebruik maken van dezelfde terminologie en vereisten om diverse interpretatie en onduidelijkheid te voorkomen. Daarnaast ziet het kabinet mogelijkheden tot het verbeteren van informatiedeling zoals voorgesteld door de Commissie. Het voorstel voorziet in een mogelijkheid voor informatiedeling, zowel tussen bedrijven, maar ook tussen de verschillende nationale toezichthouders. Op deze manier zouden dreigingen sneller bekend kunnen worden bij de toezichthouder, en kan men gebruik maken van expertise van collega-toezichthouders.

Het kabinet onderschrijft het belang dat de Commissie hecht aan een hoge mate van operationele weerbaarheid in de gehele Europese financiële sector. Het kader wat de Commissie met deze verordening voorstelt is in de ogen van het kabinet in hoofdlijnen compleet en gestoeld op de juiste principes. Het kabinet steunt de balans die de Commissie zoekt ten aanzien van het voorstel. Hoewel de verordening basisvereisten oplegt voor alle financiële instellingen, is er voldoende ruimte voor flexibiliteit. Dat wil zeggen dat kleinere bedrijven niet worden opgezadeld met onnodige (administratieve) eisen en dat ook per sector bekeken kan worden wat de risico's en bijkomende benodigde mitigerende maatregelen moeten zijn. Op deze manier zorgt de verordening voor een beter niveau van cyberweerbaarheid, maar zit het innovatie niet onnodig in de weg.

Het kabinet onderschrijft de noodzaak voor basisregels voor de gehele sector. De eisen die uit het voorstel voortvloeien ten aanzien van het inrichten van de organisatie en ICT-governance, maar ook de eisen die aan instellingen worden gesteld om significante ICT-incidenten tijdig te melden bij

de toezichthouder, ziet het kabinet als noodzakelijk. Hierbij is het van belang om de meldingsplicht helder en toepasbaar te maken, zodat bedrijven weten wanneer en waar een bepaald incident gemeld moet worden. Hierbij moet de rol van het Nationaal Cyber Security Centrum als meldpunt voor aanbieders van essentiële diensten wel geborgd blijven. Ook de eis voor de meeste partijen om jaarlijks een basistest te doen van de ICT-systemen ziet het kabinet als een nuttige toevoeging aan het regelgevend kader.

Daarnaast geeft de verordening een belangrijke rol aan TLPT, waarbij instellingen op basis van actuele dreigingsinformatie geavanceerde (ethische) hacktesten ondergaan om de eigen systemen te testen tegen cyberdreigingen. Het kabinet is verheugd dat deze geavanceerde en effectieve techniek, die in Nederland reeds met succes wordt toegepast, verplicht wordt gesteld voor significante financiële instellingen in de gehele Unie. Het Commissievoorstel vereist verder dat lidstaten elkaars TLPT erkennen. Dit zet een bepaalde kwaliteitsstandaard en maakt dat financiële instellingen zich nog maar in één lidstaat hoeven te laten testen, wat duplicatie voorkomt. Evenwel is belangrijk dat duidelijker voor een specifieke gezamenlijke TLPT-standaard wordt gekozen, om een gelijk speelveld te bewaken. Het kabinet zal er daarom bij de Commissie op aandringen om de TIBER-EU-standaard als uitgangspunt te hanteren voor TLPT in plaats van, zoals nu in de conceptverordening voorgesteld, de uitwerking van een nieuwe standaard door de Europese toezichthoudende autoriteiten (European Supervisory Authorities - ESA's). Daarbij is van belang dat alle nationale raamwerken van de lidstaten reeds op TIBER-EU zijn gestoeld.

Het kabinet steunt het feit dat de Commissie oog heeft voor de rol van derde dienstverleners. Het kabinet onderschrijft het principe dat financiële instellingen in beginsel zelf verantwoordelijk zijn en blijven voor de processen die zij uitbesteden, maar onderkent ook het belang dat zij in staat worden gesteld om bepaalde rechten op dit gebied af te dwingen bij grote kritische derde dienstverleners, zoals aanbieders van clouddiensten, door middel van de verplichte standaard contractclausules die uit het voorstel voortvloeien, alsmede dat op die dienstverleners een passend toezichtkader van toepassing is. Hierbij zou het kabinet evenwel willen zien dat deze partijen ook gehouden kunnen worden deel te nemen aan TLPT-exercities die bepaalde financiële instellingen periodiek moeten ondergaan. De bereidheid daartoe blijkt namelijk lang niet altijd te bestaan.

Mede daarom kijkt het kabinet met interesse naar het voorstel van de Commissie om een toezichtkader op te stellen voor kritische digitale derde dienstverleners. Hoewel het kabinet op hoofdlijnen het idee voor dit kader steunt, en de noodzaak ziet voor een directe rol van de (financiële) toezichthouder bij deze instellingen vanwege de toenemende risico’s voor de financiële stabiliteit die zij vormen, heeft het kabinet naar aanleiding van het Commissievoorstel nog enige vragen. Zo is de definitie van de partijen die onder dit toezichtkader zouden vallen dermate ruim dat onduidelijk is om wat voor partijen het nu precies gaat. Ook al geeft de Commissie aan dat de NIB richtlijn in stand blijft, zijn er wel degelijk vragen over hoe deze verordening zich verhoudt tot de NIB-richtlijn en de uitvoeringsverordening voor digitale dienstverleners. Momenteel is het toezicht op clouddienstverleners belegd bij het Agentschap Telecom, op grond van de NIB-richtlijn. Het kabinet is dan ook van plan om de Commissie te vragen om toe te lichten hoe DORA en de

NIB-richtlijn (inclusief uitvoeringsverordening) samen gaan, met name ten aanzien van de mogelijke overlap in het toezicht op clouddiensten.

Voorts heeft het kabinet vragen over de precieze bevoegdheden die de toezichthouders daadwerkelijk krijgen, aangezien deze beperkt lijkt tot het afgeven van niet-bindende aanbevelingen aan de derde partij. Tenslotte geeft de Commissie aan dat het toezicht op deze partijen primair op Unieniveau wordt belegd, met een belangrijke rol voor nationale toezichthouders, waarbij afhankelijk van de markt waarin de derde dienstverlener opereert, het toezicht belegd kan worden bij de Europese Bankautoriteit (EBA), de Europese Effecten- en Marktenautoriteit (ESMA) of de Europese Autoriteit voor Verzekeringen en Bedrijfspensioenen (EIOPA). Hoewel het kabinet de belangrijke rol voor een Unietoezichthouder onderschrijft, rijst de vraag of het niet efficiënter en effectiever is om de coördinatie van het toezicht bij één van de bestaande autoriteiten te beleggen en daar de expertise en kennis te verzamelen. Een belangrijke kanttekening bij het voorstel is dat het kabinet de huidige voorgestelde termijn waarbinnen de verordening van toepassing wordt niet haalbaar acht en dan ook pleit voor een verruimde termijn van 30 maanden.

c) Eerste inschatting van krachtenveld

Het voorstel wordt overwegend positief ontvangen. Vrijwel alle lidstaten zien de voordelen en de noodzaak van een geharmoniseerd Uniekader voor digitale weerbaarheid. Wel zijn verschillende opvattingen over hoe ver deze maatregelen gaan. Lidstaten waarin de financiële sector minder digitaal ontwikkeld is hechten groot belang aan de uitvoerbaarheid van de regelgeving en geven aan dat de regels op sommige punten te ver gaan. Verder lijkt de discussie zich te concentreren op het toezichtkader voor derde dienstverleners. Waar sommige lidstaten pleiten voor vergaande directe bevoegdheden voor de toezichthouders ten aanzien van deze derde dienstverleners, stellen andere lidstaten juist dat moet worden gewaakt voor overregulering. Het EP heeft zich tot dusverre nog niet uitgesproken over de verordening.

4. Beoordeling bevoegdheid, subsidiariteit en proportionaliteit

a) Bevoegdheid

De voorgestelde rechtsbasis van het voorstel is artikel 114 VWEU. Dit artikel geeft de EU bevoegdheid om maatregelen te treffen die de werking van de interne markt betreffen. Het voorstel heeft tot doel de belemmeringen voor grensoverschrijdende bedrijfsvoering te verminderen door standaarden te harmoniseren en de regels voor verschillende soorten bedrijven gelijk te trekken. Het kabinet kan zich vinden in deze rechtsbasis.

b) Subsidiariteit

Het kabinet beoordeelt de subsidiariteit van het voorstel als positief. Het grensoverschrijdende en onderling verweven karakter van de financiële sector maakt dat het wenselijk is dat op EU-niveau gehandeld wordt. Verschillen in regelgeving per lidstaat kunnen grote gevolgen hebben voor financiële entiteiten die grensoverschrijdend actief zijn of juist willen uitbreiden over grens, o.a.

vanwege hoge kosten om aan regelgeving te voldoen en dubbele rapportageverplichtingen. Het ICT-governance kader voor financiële instellingen is daardoor zeer versnipperd. Dit maakt effectief toezicht houden moeilijk, en leidt tot inconsistenties in wet- en regelgeving tussen lidstaten, en onnodige kosten voor de sector. Daarom is optreden op het niveau van de Unie gewenst.

c) Proportionaliteit

Het kabinet beoordeelt de proportionaliteit van het voorstel als positief. De Commissie kiest voor een verordening. Dit is in de ogen van het kabinet de meest effectieve oplossing om tot een gelijk speelveld in de Unie te komen en ondersteunt de ontwikkeling van een grote interne markt waarin marktpartijen zich kunnen bewegen. Een verordening voorkomt hierbij eventuele verschillen in de implementatie van regelgeving die kunnen optreden bij een richtlijn.

Het kabinet beoordeelt ook de inhoud van het voorstel als proportioneel. De risico's van cyberaanvallen en ICT-falen zijn in de laatste jaren toegenomen door de verdere digitalisering van de sector, net als de potentiele maatschappelijke effecten van een incident. Dit voorstel kan de sector in het geheel weerbaarder maken tegen deze risico's. Minder vergaande alternatieven zouden volgens het kabinet geen recht doen aan het belang van deze weerbaarheid. Hoewel de verordening basisvereisten oplegt voor alle financiële instellingen, is er voldoende ruimte voor flexibiliteit. Het voorstel beoogt rekening te houden met de grootte, het risicoprofiel en het systeembelang van partijen bij het stellen van eisen, waardoor er geen buitensporige eisen worden opgelegd aan kleinere partijen.

5. Financiële implicaties, gevolgen voor regeldruk en administratieve lasten

a) Consequenties EU-begroting

De Commissie voorziet dat kosten zullen worden gemaakt bij het instellen van nieuwe toezichtstaken. Dit omvat 18 fte bij de Europese Bankautoriteit (EBA), Europese Autoriteit voor effecten en markten (ESMA) en Europese toezichthouder van de verzekeraars en pensioenfondsen (EIOPA). Voor de ESA's worden additionele kosten voor IT, inspecties en vertalingen verwacht. Dit leidt tot een geschatte kostenimpact van 30,19 miljoen euro voor de periode 2022-2027. Deze kosten worden gedekt door de sector, middels toezichtkosten. De Commissie verwacht daarom geen consequenties voor de EU-begroting.

Voor zover deze er wel blijken te zijn, is het kabinet van mening dat de benodigde EU-middelen gevonden dienen te worden binnen de in de Raad afgesproken financiële kaders van het MFK 2014-2020 en het MFK 2021-2027, en dat deze moeten passen bij een prudente ontwikkeling van de jaarbegroting.

b) Financiële consequenties (incl. personele) voor rijksoverheid en/ of decentrale overheden

Lidstaten dienen toezichthouders aan te wijzen die toezien op de naleving van de verordening. Hoewel het kabinet hier nog geen definitief besluit over heeft genomen, ligt het in de rede om dit

toezicht te beleggen bij de AFM en/of DNB. AFM en DNB houden reeds toezicht op, onder meer, de digitale huishouding van financiële instellingen en hebben hiervoor al aanzienlijke kennis in huis. Of, en zo ja in welke mate, deze toezichthouders meer middelen nodig hebben voor het toezicht op deze verordening hangt af van de uiteindelijke vormgeving van deze verordening. Uit de Wet bekostiging financieel toezicht (Wbft) volgt dat partijen die onder toezicht staan van de AFM en/of DNB dit zelf bekostigen. In deze situatie zijn de gevolgen voor de rijksoverheid dus zeer beperkt. Eventuele budgettaire gevolgen worden ingepast op de begroting van het beleidsverantwoordelijk departement, conform de regels van de budgetdiscipline.

c) Financiële consequenties (incl. personele) voor bedrijfsleven en burger

Een algemene inschatting voor de kosten voor de naleving van de verordening door financiële instellingen is lastig te maken, aangezien in de verordening een aanpak is gekozen die rekening houdt met de aard van de dienstverlening en de grootte van de gereguleerde instelling, en de risico's die hiermee gepaard gaan. Per dienst en per dienstverlener zullen de nalevingslasten dus sterk verschillen. De nieuwe regelgeving en de eigen vermogenseis die in bepaalde gevallen geldt zal extra kosten met zich meebrengen voor marktpartijen. Deze eisen moeten volgens het kabinet proportioneel zijn om niet onnodig innovatie te belemmeren.

d) Gevolgen voor regeldruk/administratieve lasten voor rijksoverheid, decentrale overheden, bedrijfsleven en burger

De vereisten die de verordening oplegt aan financiële instellingen ten aanzien van hun ICT-huishouding, zullen voor sommige partijen leiden tot verhoogde lasten en regeldruk. Het is nog moeilijk om in te schatten hoe groot deze verhoging is, omdat veel van de technische standaarden later zullen worden vastgesteld. Een aantal van de voorgestelde eisen is in Nederland reeds staand beleid, wat de toename van lasten en regeldruk beperkt.
Anderzijds zal het harmoniseren van de vereisten de kosten voor grensoverschrijdend opererende instellingen verlagen, omdat verschillen tussen lidstaten worden weggenomen. Ook het erkennen van testen tussen landen zal de regeldruk en lasten verminderen, omdat deze tests niet opnieuw hoeven te worden uitgevoerd.

e) Gevolgen voor concurrentiekracht

Er is weinig bekend over de mogelijke gevolgen voor concurrentiekracht. Het kan worden aangenomen dat een weerbaardere, veiligere sector minder gevoelig is voor cyberincidenten. Dit komt de financiële stabiliteit ten goede en zal leiden tot een verlaging van de maatschappelijke kosten die dit soort incidenten met zich meebrengen. Dit komt de concurrentiekracht van de financiële sector ten goede. Hiernaast zullen minder bedrijven individueel kosten maken voor het oplossen van de gevolgen van dit soort incidenten. Dit zal naar verwachting in verhouding staan met de extra gemaakte individuele kosten van bedrijven.

6. Implicaties juridisch

a) Consequenties voor nationale en decentrale regelgeving en/of sanctionering beleid (inclusief toepassing van de lex silencio positivo)

Het betreft een verordening en deze heeft directe werking in de Nederlandse rechtsorde. Veel reeds bestaande bepalingen die via sectorale richtlijnen geïmplementeerd zijn in nationale wetgeving worden overgeheveld naar de verordening. Dit betekent dat aanpassingen aan nationale wetgeving nodig zijn.

De verordening schrijft verder voor dat er een nationale toezichthouder moet worden aangewezen om toezicht uit te oefenen op de naleving van de eisen uit de verordening. Zoals eerder aangegeven ligt het in de rede dat dit in Nederland wordt belegd bij de AFM en DNB, die thans reeds een toezichthoudende verantwoordelijkheid hebben op dit gebied, en dat dit middels een aanpassing van een besluit wettelijk geregeld kan worden.

b) Gedelegeerde en/of uitvoeringshandelingen, incl. NL-beoordeling daarvan

Op verschillende plekken in de Verordening wordt de bevoegdheid aan de Commissie gedelegeerd om technische standaarden vast te stellen. Het gaat hier om:

- Art. 14: het vaststellen van technische standaarden voor ICT-veiligheidsbeleid, methodes en processen.
- Art. 16: het classificeren van ICT-gerelateerde incidenten.
- Art. 18: harmonisering van rapportage-eisen.
- Art. 23: een kader voor intelligence-based penetration testing.
- Art. 25: het maken van templates voor een informatieregister voor contracten met derde partijen.
- Art. 27: het vaststellen van standaardclausules voor het uitbesteden van kritieke of belangrijke diensten.
- Art. 38: het aanvullen van criteria voor het benoemen van kritieke derde partij ICT-aanbieders
- Art. 36: het harmoniseren van eisen om toezicht te kunnen voeren op kritieke derde partij ICT-aanbieders
- Art. 38: het vaststellen van toezichtkosten van kritieke derde partij ICT-aanbieders

De uitoefening van de gedelegeerde bevoegdheid door de Commissie wordt in art. 50 uitgewerkt voor wat betreft de bevoegdheid verleend in artikel 38 lid 5 en artikel 28 lid 3. Voor de overige gedelegeerde bevoegdheden gaat het voornamelijk om het aannemen van technische standaarden die de Commissie door de ECB, EBA, ESMA, of EIOPA wil laten voorbereiden, de uitoefening van die bevoegdheden wordt uitgeoefend in overeenstemming met de basisverordeningen die zien op de ECB, EBA, ESMA of EIOPA. Het kabinet kan zich vinden in de verleende gedelegeerde bevoegdheden omdat het hier de technische uitwerking van bepaalde eisen en formats betreft. Dergelijke technische standaarden dienen ter aanvulling of wijziging van niet essentiële onderdelen

van de verordening. Ten slotte betreffen de gedelegeerde bevoegdheden voor een deel vergelijkbare bevoegdheden die de Commissie reeds heeft bij andere verordeningen en richtlijnen.

c) Voorgestelde implementatietermijn (bij richtlijnen), dan wel voorgestelde datum inwerkingtreding (bij verordeningen en besluiten) met commentaar t.a.v. haalbaarheid

De Verordening is van toepassing 12 maanden na inwerkingtreding, met uitzondering van art. 23 en 24, die regels stellen voor geavanceerde testen en eisen stellen voor testers. Deze artikelen zijn 36 maanden na inwerkingtreding van toepassing.

Aangezien er met deze verordening en de bijbehorende richtlijn aanpassingen plaats vinden aan verschillende richtlijnen, die weer in nationale wetgeving is geïmplementeerd, acht het kabinet de termijn het niet haalbaar

d) Wenselijkheid evaluatie-/horizonbepaling

In art. 51 stelt de Commissie voor om 5 jaar na inwerkintreding een evaluatie uit te voeren en indien nodig nieuwe wetgevende voorstellen in te dienen. Het kabinet kan zich vinden in dit tijdspad.

e) Constitutionele toets

Niet van toepassing

7. Implicaties voor uitvoering en/of handhaving

a. Uitvoerbaarheid

De uitvoering van de Verordening is veelal aan de financiële instellingen, die ICT-systemen dienen te onderhouden en incidenten dienen te rapporteren. De toezichthouder zal echter wel een rol spelen bij de geavanceerde TLPT-exercities die significante instellingen moeten ondergaan. De bestaande kennis en kunde die binnen de toezichthouder en bij de financiële instellingen aanwezig is, maakt dat Nederland vertrouwen heeft in de uitvoerbaarheid van het voorstel.

b. Handhaafbaarheid

Veel van de uitvoering van de eisen ligt bij financiële instellingen, maar het toezicht hierop wordt gehouden door nationale en Europese toezichthouders. Zoals eerder aangegeven ligt het in de rede om, hoewel het kabinet meer tijd nodig heeft om hier een definitief besluit over te nemen, de AFM en DNB aan te wijzen als nationale toezichthouders. Sommige partijen zullen onder Europees toezicht vallen, wat in veel gevallen goed te verantwoorden is. Bij één punt zien we echter mogelijke complicaties, namelijk het toezicht op kritieke derde partij ICT-dienstverleners. Dit toezicht wordt afhankelijk van de activiteiten gedaan door EBA, ESMA of EIOPA. In een situatie waarin de dienstverlener diensten aan verschillende soorten financiële instellingen verleent, is het op dit moment nog niet goed te overzien hoe de toezichthouder het toezicht effectief kan uitvoeren. Nederland zal hier vragen om toelichting van de Commissie.

8. Implicaties voor ontwikkelingslanden

Geen implicaties voor ontwikkelingslanden