DeNederlandscheBank
EUROSYSTEEM

Aangetekend met bericht van ontvangst

Ministerie van Financiën
Postbus 20201
2500 EE Den Haag

De Nederlandsche Bank N.V.

Postbus 98
1000 AB Amsterdam
+31 20 524 91 11
www.dnb.nl

Handelsregister 3300 3396
BTW: NL003569056B01

Onderwerp
Uitvoeringstoets inzake het uitvoeringsbesluit DORA

Datum
20 juni 2024

Uw kenmerk
2024-0000173518

Ons kenmerk
T027-1645043135-5872

Behandeld door

Telefoonnummer

Mailadres

Geachte,

Naar aanleiding van het verzoek in uw brief met kenmerk 2024-0000173518, heeft DNB een uitvoerings- en handhaafbaarheidstoets uitgevoerd op het *uitvoeringsbesluit DORA*.[1]

Per 17 januari 2025 zal de *Digital Operational Resilience Act* (DORA) van toepassing zijn. DORA betreft een Europese verordening die sectorbrede geharmoniseerde vereisten opstelt voor financiële instellingen ten aanzien van ICT-risicobeheer, ICT-uitbesteding, rapportage van ICT-gerelateerde incidenten en cyberdreigingen, en het uitvoeren van testen van digitale operationele weerbaarheid, waaronder geavanceerde *threat-led penetration testing* (TLPT). Ook introduceert DORA een *oversightkader* voor kritieke ICT-dienstverleners, die door financiële instellingen worden gebruikt ten behoeve van hun financiële dienstverlening.

Ik verwacht dat het uitvoeringsbesluit DORA zal leiden tot een aanzienlijke extra vereiste inspanning voor DNB, die ook implicaties zal hebben voor de toezichtkosten. Hieronder volgt een inschatting hiervan. Deze inschatting voor DORA is ook opgenomen in het Kostenkader DNB 2025 - 2028.[2]

Uitvoering
Tot 2025 is geen verzoek voor additionele middelen opgenomen. Dit betekent echter niet dat de aanloop naar de invoering van DORA geen extra inzet vergt. Er is reeds sprake van aanzienlijke inzet van beleidsmedewerkers, experts binnen zowel het uitvoerend toezicht als de centrale bank en IT-medewerkers. Deze inzet is gericht op het opstellen van de implementatieregelgeving, de interne voorbereiding en de implementatie van DORA. Deze inzet zal binnen de bestaande kaders worden ingevuld, al vergt dit wel herprioritering van andere werkzaamheden.

In het uitvoeringsbesluit DORA wordt DNB via bijlage 35 aangewezen als bevoegde autoriteit voor *betaaldienstverleners met zetel in een andere lidstaat of betaaldienstverleners die geheel of gedeeltelijk zijn vrijgesteld van artikel 2:3a, eerste lid, van de wet.* DNB verzoekt om een aanpassing van deze bepaling in het uitvoeringsbesluit. Betaaldienstverleners met zetel in een andere lidstaat staan onder toezicht van de toezichthouder in die lidstaat, DNB kan daarom niet worden aangewezen als verantwoordelijk toezichthouder voor deze instellingen. Wij stellen voor de bepaling te wijzigen in: *betaaldienstverleners die geheel of gedeeltelijk zijn vrijgesteld van artikel 2:3a, eerste lid, van de wet en actief zijn in Nederland.* Deze wijziging waarborgt dat DNB binnen haar toezichtsbevoegdheden kan opereren en er geen overlap in bevoegdheden ontstaat met toezichthouders in andere lidstaten.

[1] Besluit tot wijziging van het Besluit EU-verordeningen Wft en enkele andere besluiten in verband met Verordening (EU) 2022/2554 en Richtlijn (EU) 2022/2556 betreffende digitale operationele weerbaarheid voor de financiële sector (Uitvoeringsbesluit verordening digitale operationele weerbaarheid)
[2] https://open.overheid.nl/documenten/2ef1b448-6250-47b8-be67-e356215b7a7e/file

DeNederlandscheBank
EUROSYSTEEM

Datum
20 juni 2024

Ons kenmerk
T027-1645043135-5872

DNB verwacht ook voor pensioenfondsen te worden aangewezen als bevoegde autoriteit onder DORA middels een aanpassing van de Pensioenwet waarin het prudentieel toezicht op pensioeninstellingen is geregeld. Omdat het DORA-toezicht sectoroverstijgend is, is onderstaand ook de verwachte FTE-impact voor pensioenfondsen opgenomen.

De bekostiging van de taken die voortvloeien uit DORA ten behoeve van centrale effectenbewaarinstellingen en centrale tegenpartijen zijn niet opgenomen. Voor deze instellingen wordt verzocht een uitzondering in de Wet bekostiging financieel toezicht 2019 toe te voegen.

Bij het van kracht worden van DORA – per januari 2025 – verwacht DNB additionele middelen nodig te hebben om de nieuwe verantwoordelijkheden te kunnen uitvoeren. De huidige inschatting van benodigde additionele middelen betreft een structureel aantal (op jaarbasis) van 10,5 FTE's voor de periode 2025-2026; en 12,5 FTE's vanaf 2027.

Naast de benodigde additionele FTE's zoals hierboven aangegeven, verwacht ik dat onder DORA de financiering van 4,5 bestaande FTE's vanaf 2025 via de ZBO-begroting zal verlopen, in plaats van via de huidige directe financiering. Het gaat om FTE's die ingezet zullen worden ten behoeve van TLPT-testing. Dit betreft de doorberekening aan de ZBO-begroting van ca. 30% van de kosten van de afdeling die TLPT-testen uitvoert.[3] De mogelijkheid tot directe doorberekening van de kosten van de huidige (vrijwillige) TIBER-testen aan de TIBER-deelnemers komt immers te vervallen wanneer zij onder DORA worden aangewezen voor het verplicht uitvoeren van een TLPT.

DNB zal door de Europese Toezichthoudende Autoriteiten (ETA's) ook worden gevraagd capaciteit te leveren voor het *oversightkader* op kritieke ICT-dienstverleners (*critical third-party providers*, CTPP's). DNB verwacht hiervoor 2 FTE's te leveren. De kosten voor deze FTE's worden direct doorberekend aan de CTPP's, waardoor deze capaciteit geen financiering behoeft via de ZBO-begroting en dus niet is opgenomen in tabel 1.[4]

Onderstaande tabel geeft een overzicht van de benodigde middelen, bijlage 1 bevat een verdere gedetailleerde uitsplitsing naar DORA-gerelateerde activiteiten.

Centrale bank begroting		
Begroting	*Benodigd #FTE*	*Toelichting*
Totaal aantal additionele FTE's vanaf 2025	-4,5	Dit aantal betreft de FTE's voor TLPT die overgeheveld worden naar de ZBO-begroting.
ZBO-begroting		
Begroting	*Benodigd #FTE*	*Toelichting*
Totaal aantal additionele FTE's (vanaf 2025) Totaal aantal additionele FTE's (vanaf 2027) Verschuiving doorbelasting van centrale bank naar ZBO (geen additionele FTE's)	10,5 12,5 4,5	

[3] Het betreft de afdeling Cyber- Beleid, -Intelligence en TIBER testen (C-BIT), onderdeel van de Divisie Betalingsverkeer en Marktinfrastructuur.
[4] https://www.eiopa.europa.eu/publications/joint-esas-response-call-advice-specifying-further-criteria-critical-ict-third-party-service_en

DeNederlandscheBank
EUROSYSTEEM

Datum
20 juni 2024

Ons kenmerk
T027-1645043135-5872

Totaal		
Begroting	*Benodigd #FTE*	*Toelichting*
Totaal additionele FTE's voor rekening van **ZBO-begroting** (vanaf 2025)	15	Dit betreft het totaal aantal FTE's dat additioneel is en ten laste zal komen van de ZBO-begroting, inclusief bestaande FTE's voor TLPT die onder DORA gefinancierd dienen te worden via de ZBO-begroting.
Totaal additionele FTE's voor rekening van **ZBO-begroting** (vanaf 2027)	17	
Totaal additioneel (**Centrale Bank én ZBO begrotingen tezamen**) (vanaf 2025)	10,5	
Totaal additioneel (**Centrale Bank én ZBO begrotingen tezamen)** (vanaf 2027)	12,5	

Tabel 1 – Overzicht additionele middelen t.b.v. uitvoering DORA

Het betreft FTE's op (senior) medewerker niveau; de inschatting is dat additionele middelen op managementniveau (afdelingshoofd, divisiedirecteur) niet nodig zijn.

DNB houdt al geruime tijd toezicht op de ICT- en operationele risico's van financiële instellingen. DORA is echter op veel gebieden uitgebreider, gedetailleerder en dwingender dan bestaande *guidelines* en *good practices*. De implementatie van DORA in onze toezichtorganisatie vereist dan ook zowel de aanscherping van bestaande toezichtprocessen als de inrichting van nieuwe processen. De additionele FTE's komen voornamelijk voort uit:

- De opvolging van rapportages die worden verkregen onder de DORA-regelgeving, met name rapportages ten aanzien van ICT-incidenten, het informatieregister m.b.t. uitbestedingen, informatie-uitwisseling over incidenten tussen toezichthouders, en bevindingen die gerapporteerd worden in het kader van geavanceerde testen (TLPT);
- Additionele en bindende vereisten voor pensioenfondsen en verzekeraars op het gebied van ICT-risicomanagement en *third-party risicomanagement* (uitbesteding);
- Een uitbreiding van het aantal instellingen dat geavanceerde tests van digitale operationele weerbaarheid (TLPT) moet uitvoeren ten opzichte van de vergelijkbare huidige vrijwillige TIBER-testen;

Ik hecht eraan te onderstrepen dat bovengenoemde inschattingen onderhevig zijn aan onzekerheden. Zo bestaat er onzekerheid over hoe het DORA-toezicht in de praktijk zal uitwerken en zijn er parallelle ontwikkelingen, zoals de invoering van de MiCAR-regelgeving voor crypto-dienstverleners en de pensioentransitie, die impact kunnen hebben op het toezichtlandschap.

Handhaving
Ik voorzie geen significante obstakels in de handhaving van DORA. DORA legt bindende en specifieke eisen op aan financiële instellingen ten aanzien van ICT-gerelateerd risicobeheer. Ten opzichte van de huidige situatie ontstaat hiermee een grotere rol voor formele handhavingsinstrumenten; het is daarmee van belang dat DNB beschikt over een afdoende en voldoende-flexibel handhavingsinstrumentarium. Dit wordt voldoende geadresseerd in het uitvoeringsbesluit DORA.

Tot slot wil ik aangeven dat DORA-regelgeving niet direct van toepassing zal zijn op pensioenuitvoeringsorganisaties (PUO's): entiteiten die administratiediensten leveren aan pensioenfondsen. Hoewel onder de DORA-regelgeving PUO's als interne dan wel externe dienstverlener gelden, zijn zij geen financiële entiteiten en zullen als zodanig niet onder bindende DORA-vereisten vallen. DNB zal het bestaande PUO-gerichte toezicht voortzetten. DNB zal de ontwikkelingen in het kader van o.a. de

DeNederlandscheBank
EUROSYSTEEM

pensioentransitie blijven volgen om vast te stellen of een wettelijke basis voor bindende vereisten voor PUO's ten aanzien van ICT-risicobeheer in de toekomst gewenst is.

Datum
20 juni 2024

Ons kenmerk
T027-1645043135-5872

Hoogachtend,

DeNederlandscheBank
EUROSYSTEEM

Bijlage 1 – Overzicht additionele middelen DORA

Opvolging meldingen ICT-incidenten		
Type(n) financiële entiteiten	*#FTE benodigd*	*Toelichting*
Alle typen financiële entiteiten onder DORA-toezicht van DNB	0,75 FTE	DORA vereist dat alle typen financiële entiteiten ernstige ICT-gerelateerde incidenten rapporteren. Dit betreft een nieuwe verplichting voor vooral verzekeraars en pensioenfondsen, waardoor een toename in het aantal meldingen wordt verwacht. Daarnaast verwacht DNB onder DORA ook meer gestructureerde opvolging te zullen (moeten) geven aan deze incidenten.
Opvolging (TLPT-)test bevindingen		
Type(n) financiële entiteiten	*#FTE benodigd*	*Toelichting*
Alle typen financiële entiteiten onder DORA-toezicht van DNB die geavanceerde testen (TLPT) moeten ondergaan	0,5 FTE	DORA vereist dat toezichthouders opvolging geven aan bevindingen (verbeterpunten) die voortkomen uit de testen van financiële entiteiten. Dit betreft additionele toezichtactiviteiten.
Registers of Information (uitbestedingsregisters)		
Type(n) financiële entiteiten	*#FTE benodigd*	*Toelichting*
Alle typen financiële entiteiten onder DORA-toezicht van DNB	0,75 FTE	DORA vereist tenminste jaarlijkse uitvraag van uitbestedingsregisters en aggregatie door toezichthouders.
Toezicht vereisten ICT- & Third-Party Risicomanagement		
Type(n) financiële entiteiten	*#FTE benodigd*	*Toelichting*
Pensioenfondsen en verzekeraars	4,5 FTE's	DORA zorgt voor een verschuiving van open normen naar stringente wettelijke kaders voor het beheersen en toezien op de beheersing van IT-risico's. In het bijzonder voor de pensioensector, waar het toezicht nu is vormgegeven op basis van een eigen interpretatie van beheerste en integere bedrijfsvoering. Dit geldt in mindere mate voor de verzekeringssector, waar enige wettelijke basis wordt gelegd door Solvency II. Voor overige entiteiten (banken, betaalinstellingen, elektronisch-geldinstellingen, centrale tegenpartijen, centrale bewaarinstellingen) is de inschatting dat DORA op het terrein van ICT- en Third-Party risicomanagement slechts in beperkte mate additionele vereisten oplegt t.o.v. geldende regelgeving. Ik verwacht daarom voor deze instellingen deze vereisten binnen het bestaande toezicht te kunnen absorberen.

DeNederlandscheBank
EUROSYSTEEM

Begeleiden Threat-Led Penetration Testing (TLPT)		
Type(n) financiële entiteiten	*#FTE benodigd*	*Toelichting*
Alle typen (financiële) instellingen onder DNB DORA-toezicht die geavanceerde testen (TLPT) moeten ondergaan	Additioneel vanaf 2025: 2 FTE's Additioneel vanaf 2027: 4 FTE's Doorbelasting bestaande FTE naar ZBO: 4,5 FTE's	Onder DORA zullen ook geselecteerde (ICT-) dienstverleners van financiële entiteiten meegenomen moeten worden in de TLPT-test, hetgeen een uitbreiding van de testscope betekent. Daarnaast dienen ook buitenlandse bijkantoren van Nederlandse entiteiten worden meegenomen in TLPT-testen (scope-uitbreiding) en zal bijgedragen moeten worden aan testen van Nederlandse bijkantoren/operaties van buitenlandse financiële entiteiten. Gegeven de onzekerheid over langere-termijn ontwikkelingen, dient de 2 FTE's te worden gezien als een inschatting voor 2025 - 2026, met de inschatting dat er vanaf 2027 nog eens 2 FTE's nodig zullen zijn. N.B.: omdat TLPT testing onder DORA een toezichtverplichting wordt, wordt tevens voorgesteld om 30% van BVM C-BIT capaciteit volgens de begroting van 2025 gericht op TLPT-testen via de ZBO-begroting te financieren in plaats van de huidige rechtstreekste financiering door geteste instellingen. Dit betreft doorbelasting van ca. 4,5 FTE's.
Juridisch advies, handhaving en beleidsontwikkeling		
Type(n) financiële entiteiten	*#FTE benodigd*	*Toelichting*
Alle typen financiële entiteiten onder DORA-toezicht van DNB	1 FTE	Om de cross-sectorale en uniforme toepassing van DORA op Europees niveau te waarborgen verwacht ik een continuering van de beleidsinzet. Deze zal zich o.a. richten op de ontwikkeling van een pan-Europees *Systemic Cyber Incident Coordination Framework* (EU SCICF), bijdragen aan verdere beleidsinvulling en interpretatie van de wetgeving, en vertegenwoordiging in Europese gremia.
Alle typen financiële entiteiten onder DORA-toezicht van DNB	1 FTE	Om de juridische ondersteuning bij de toepassing en handhaving van DORA te kunnen waarborgen wordt uitgegaan van een meegroeimodel van 10%. Dit staat ons toe om waar nodig DORA ook formeel te handhaven. Voorheen was hiervan beperkt sprake omdat de basis van het ICT-toezicht werd gevormd door *good practices* en *guidelines*.

Datum
20 juni 2024

Ons kenmerk
T027-1645043135-5872

DeNederlandscheBank
EUROSYSTEEM

Toezicht (*oversight*) Cruciale ICT-dienstverleners		
Type(n) financiële entiteiten	*#FTE benodigd*	*Toelichting*
Cruciale ICT-dienstverleners (CTPP)	2 FTE's – financiering via de CTPP's	Het oversight op CTPP's kent veel onzekerheden. De inrichting wordt nog vormgegeven, en het aantal daadwerkelijk aan te wijzen CTPP's nog onbekend. Op basis van een analyse voor de Nederlandse markt is ervanuit gegaan dat AFM en DNB in totaal zullen bijdragen aan oversight op 6 – 10 CTPP's (via lidmaatschap van Joint Examination Teams, JETs). Uitgaande van 50-50 verdeling tussen AFM en DNB en een behoefte van 0,5 FTE per JET, komt dit neer op 1,5 – 2,5 FTE's voor DNB. N.B.: deze FTE's worden gefinancierd middels doorberekening aan de CTPP's en behoeven daarom geen financiering van de financiële sector danwel het Ministerie. Deze FTE's zijn dan ook niet meegeteld in het verzoek.

Datum
20 juni 2024

Ons kenmerk
T027-1645043135-5872