

Vergaderjaar 2023–2024

36 526

Wijziging van de Wet ter voorkoming van witwassen en financieren van terrorisme en enige andere wetten in verband met de uitvoering van Verordening (EU) 2023/1113 betreffende bij geldovermakingen en overdrachten van bepaalde cryptoactiva te voegen informatie en tot wijziging van Richtlijn (EU) 2015/849 (Uitvoeringswet verordening bij geldovermakingen en overdrachten van cryptoactiva te voegen informatie)

Nr. 7

NOTA NAAR AANLEIDING VAN HET VERSLAG

Ontvangen 10 september 2024

Inleiding

De regering is de vaste commissie voor Financiën erkentelijk voor de aandacht die zij aan het onderhavige wetsvoorstel heeft geschonken en voor de door haar daarover gestelde vragen. De vragen worden zo veel mogelijk beantwoord in de volgorde van het door de commissie uitgebrachte verslag. Voor zover vragen, vanwege overeenkomst in onderwerp, gezamenlijk beantwoord zijn, is dit vermeld.

Algemeen

§ 1. Inleiding

De leden van de NSC-fractie vragen wat het verschil is tussen de inwerkingtreding (30 juni 2023) en van toepassing zijn (30 december 2024).

In Nederlandse wetgeving is het tijdstip van inwerkingtreding van een regeling vaak ook het moment waarop de in die regeling opgenomen materiële normen gaan gelden. In EU-wetgeving vallen die momenten meestal niet samen. Standaard treedt een verordening al op de twintigste dag na publicatie in werking. De verordening maakt dan in algemene zin al wel deel uit van het EU-recht, maar hoeft dan meestal nog niet inhoudelijk te worden nageleefd. Het moment waarop een verordening ook inhoudelijk moet worden nageleefd, is het moment waarop de verordening «van toepassing» wordt. Door de verordening pas op een later tijdstip van toepassing te laten worden, wordt aan de lidstaten en aan burgers, bedrijven en instellingen voor wie de verordening gaat gelden een termijn geboden waarbinnen zij zich op de nieuwe regels kunnen voorbereiden. In Nederlandse wetgeving is het gebruikelijk om een regeling ook dan pas in werking te laten treden, waardoor inwerking-

trekking en toepassing in tijd samenvallen. Richtlijnen kennen overigens nog een derde moment: de uiterste datum waarop de lidstaten hun implementatiewetgeving ter omzetting van de richtlijn gereed moeten hebben.

De leden van de NSC-fractie vragen welke keuzemogelijkheden lidstaten nog hebben op nationaal niveau bij de implementatie.

Verordeningen bieden naar hun aard doorgaans geen ruimte voor nationaal beleid, los van specifieke lidstaattopties. Dit volgt al uit de keuze van de Europese wetgever om zelf rechtstreeks werkende voorschriften vast te stellen en dat niet, door vaststelling van een richtlijn, aan de lidstaten over te laten. Voor verordeningen geldt bovendien dat zij in beginsel uitputtend bedoeld zijn en de lidstaten geen ruimte meer bieden voor nationaal beleid, tenzij een verordening daar uitdrukkelijk in voorziet. Er zaten een aantal lidstaattopties in TFR. Deze opties waren voornamelijk formeel van aard. Er is geen gebruik gemaakt van de lidstaattoptie uit artikel 2, vijfde lid van TFR, waarin de mogelijkheid wordt geboden aan lidstaten om TFR niet van toepassing te verklaren op bepaalde groepen. Artikel 1c, eerste lid van de Wet ter voorkoming van witwassen en financieren van terrorisme (hierna: Wwft) bevat al een algemene ontheffingsgrondslag waarvan gebruik kan worden gemaakt indien het wenselijk is aan bepaalde groepen een ontheffing te verlenen van de verplichtingen van TFR. De lidstaattopties in artikel 26, tweede en derde lid van de TFR zien op langere bewaartermijnen van gegevens. Omdat dit niet nodig wordt geacht, is er geen gebruik gemaakt van deze lidstaattopties. Artikel 38, zesde lid van TFR betreft een lidstaattoptie waarvan wel gebruik wordt gemaakt. Dit gaat over het aanwijzen van een centraal contactpunt. Nu voor verschillende financiële instellingen ervoor gekozen is een centraal contactpunt aan te wijzen in Nederland is ervoor gekozen een dergelijk contactpunt ook aan te wijzen voor aanbieders van cryptoactivadiensten.

De leden van de NSC-fractie vragen wat het standpunt van de regering was in de Europese Raad inzake deze Verordening bij geldovermakingen en overdrachten van cryptoactiva te voegen informatie.

Het Nederlandse standpunt voor de raadsonderhandelingen is vastgesteld via het betreffende BNC-fiche en met de Kamer gedeeld.¹ In het fiche heeft het kabinet aangegeven positief te zijn over het voorstel. Het kabinet heeft meermaals aangegeven zich in te zetten om alle FATF-aanbevelingen² ten aanzien van crypto's zoveel mogelijk op EU-niveau te implementeren. Dit geldt in het bijzonder voor het uitbreiden van de reeds bestaande verordening door cryptoactiva en cryptoactivadienstverleners toe te voegen aan de reikwijdte van de verordening.³ Dat wordt met deze verordening bewerkstelligd. De andere inhoudelijke aandachtspunten van het kabinet ten aanzien van het oorspronkelijke voorstel, zoals beschreven in het BNC-fiche, zijn volledig of grotendeels geland in de uiteindelijke verordening, zoals een betere stroomlijning van deze verordening met de verordening markten in cryptoactiva (MiCA).

§ 2. Inhoud van de verordening

De leden van de GroenLinks-PvdA-fractie vragen of de regering nog eens kan toelichten hoe met het wegnemen van de minimis-regel smurfing (het

¹ Kamerstukken II, 2021–2022, 22 122, nr. 3205.

² <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>.

³ <https://www.rijksoverheid.nl/documenten/publicaties/2021/09/24/fiche-3-verordening-betreffende-bij-geldovermaking-te-voegen-informatie>.

onder een grenswaarde van toezicht op transacties blijven door deze transacties in brokjes op te knippen) wordt tegengegaan en dit bijdraagt aan de effectiviteit van het tegengaan van anonimiteit.

Met TFR wordt beoogd de anonimiteit van cryptotransacties tegen te gaan doordat het verplicht wordt voor alle aanbieders van cryptoactivadiensten (zoals gedefinieerd in MiCA), behalve partijen die advies geven, om bij overdrachten van cryptoactiva informatie toe te voegen over de initiator en de begunstigde, net zoals nu al het geval is voor betalingsdienstaanbieders bij geldovermakingen. De FATF-standaarden bieden ruimte om dit pas toe te passen bij transacties vanaf 1.000 euro. De FATF-standaarden stellen dat deze de-minimisregel niet geldt als het gaat om een samengestelde transactie (meerdere transacties die gezamenlijk uiteindelijk één transactie vormen).

In de praktijk is het echter lastig om duidelijk te bepalen wanneer meerdere transacties wel of niet als een samengestelde transactie gezien moeten worden. In de verordening is daarom uiteindelijk besloten om voor alle transacties tussen aanbieders van cryptoactivadiensten, ongeacht de waarde van de transactie, te eisen dat informatie wordt toegevoegd. Hierdoor wordt voorkomen dat personen om de regels heen werken door transacties op te knippen, waardoor individuele transacties onder de 1.000 euro blijven. Daar waar het gaat om de overdracht van of naar een zelfgehost adres, is de de-minimisregel wel toegepast en dient er pas bij een bedrag vanaf 1.000 euro onderzoek te worden gedaan naar de initiator of de begunstigde.

De leden van de GroenLinks-PvdA-fractie vragen voorts op welke manier deze verordening zal gaan toezien op crypto-transacties tussen een partij gelegen in de EU en een in een derde jurisdictie gelegen partij. Wordt deze laatste partij ook geïdentificeerd als onderdeel van deze verordening?

TFR is van toepassing op de overdracht van cryptoactiva waarbij een cryptodienstverlener is betrokken. Enkel cryptodienstverleners gevestigd in de EU worden gezien als aanbieders in de zin van TFR. TFR is niet van toepassing op een cryptodienstverlener gevestigd in een derde land, omdat TFR geen extraterritoriale werking heeft. Op basis van TFR geldt echter wel dat bij de overdracht van cryptoactiva vanuit de EU naar een derde land, informatie over de initiator en de begunstigde van de overdracht toegevoegd moet worden. Andersom geldt dat als cryptodienstverleners transacties ontvangen, al dan niet uit derde landen, zij moeten controleren of de op grond van TFR de vereiste gegevens zijn bijgevoegd. Indien dit niet het geval is moeten cryptodienstverleners mitigerende maatregelen treffen en kunnen transacties worden geweigerd, teruggezonden of zelfs worden opgeschort. De zakelijke relatie dient bij herhaaldelijk niet verstrekken van informatie zelfs te worden beperkt of beëindigd door de cryptodienstverlener.

De normen van TFR vloeien voort uit de aanbevelingen van de FATF en deze aanbevelingen worden in veel andere jurisdicties die lid zijn van de FATF, waaronder verschillende derde landen, geïmplementeerd.

De leden van de GroenLinks-PvdA-fractie vragen tevens welk risico op smurfing er specifiek is bij geldovermakingen van en naar self-hosted wallets (omdat hier wel een minimumbedrag van 1.000 euro geldt).

In het geval van smurfing wordt het te witwassen bedrag opgeknipt in kleinere bedragen en verspreid naar verschillende rekeningen. Op deze manier proberen criminelen onder de wettelijke rapportagemilieuten te

blijven en daarmee detectie te voorkomen. Zelfgehoste bewaarportemonnees worden volledig beheerd door een gebruiker. Hierdoor zijn transacties van een naar een dergelijk zelfgehost adres lastiger te achterhalen. Daar waar het gaat om een zelfgehost adres is er desalniettemin een grensbedrag van 1.000 euro ingevoerd. Deze grens is getrokken om enerzijds de doeltreffendheid van betalingssystemen niet te ondergraven en anderzijds om de potentiële dreiging die van kleine geldovermakingen uitgaat te ondervangen. Daarnaast zou het de facto onmogelijk worden om nog transacties van of naar zelfgehoste adressen te sturen, ook als het gaat om legitiem gebruik. Dit wordt ondervangen door extra eisen aan aanbieders van cryptoactivadiensten om, in aanvulling op de standaard cliëntenonderzoeksmaatregelen, te beschikken over interne beleidsregels, procedures en controles om het risico op het witwassen van geld en terrorismefinanciering vast te stellen en te beoordelen bij overdrachten van cryptoactiva naar of vanuit een zelfgehost adres. Zo moet de cryptoactivadienstverlener die de transactie faciliteert nagaan of dat zelfgehoste adres daadwerkelijk eigendom is van die cliënt of daadwerkelijk onder diens zeggenschap staat. Ook dienen er risicobeperkende maatregelen worden getroffen die in verhouding staan tot de vastgestelde risico's. Deze verplichtingen dragen bij aan de mitigatie van de risico's daar waar het gaat om de overdracht van en/of naar zelfgehoste bewaarportemonnees.

De leden van de NSC-fractie vragen of de TFR-verordening ook leidt tot een wijziging van de Sanctiewet. Zo ja, welke?

Met de Uitvoeringswet worden de partijen die gehouden zijn aan afdeling 5 van de Sanctiewet 1977 uitgebreid naar alle aanbieders van cryptoactivadiensten waarop de Wwft van toepassing is, waar voorheen afdeling 5 van Sanctiewet 1977 enkel van toepassing was op aanbieders van diensten voor het wisselen tussen virtuele valuta en fiduciaire valuta en van bewaarportemonnees. Hiermee wordt ervoor gezorgd dat er ook eenduidig wetgevend kader blijft bestaan voor cryptoactivadienstverleners ten aanzien van de sanctiewetgeving. Daarnaast worden cryptoactivadienstverleners ook meegenomen in de door het kabinet aangekondigde herziening van de sanctiewetgeving.

§ 4.2. Verscherpt cliëntenonderzoek

De leden van de NSC-fractie vragen op welke manier betalingen binnen het criminele circuit hiermee blootgelegd kunnen worden. Hoe waarschijnlijk is het dat criminelen hun (echte) persoonsgegevens gaan opgeven bij een cryptotransactie?

Met de implementatie van TFR komen alle cryptoactivadienstverleners onder de reikwijdte van de Wwft. Dit betekent onder andere dat deze instellingen cliëntenonderzoek moeten doen. In een cliëntenonderzoek moet de instelling de identiteit van hun klant vaststellen en kijkt een instelling of er risico's zijn dat een klant geld witwast of helpt om terrorisme te financieren. Wanneer de cryptoactivadienstverlener die een cryptoactivatransactie faciliteert niet alle benodigde informatie heeft ontvangen en de risico's niet goed kan beoordelen, of deze te hoog vindt, zou de transactie opgeschort kunnen worden of helemaal niet plaatsvinden. Dit geldt ook als er (mogelijk) sprake is van het opgeven van valse persoonsgegevens. Als cryptoactivadienstverleners hun processen voor het cliëntenonderzoek goed op orde hebben, zou het risico op het verlenen van diensten op basis van valse persoonsgegevens beperkt moeten zijn. Dit neemt niet weg dat malafide partijen altijd op zoek zullen zijn naar mogelijkheden om de regels te ontwijken. Daarom is het van belang dat

cryptodienstverleners hun zaken op orde hebben en dat er goed toezicht op ze wordt gehouden.

§ 4.4. Toezichthoudende autoriteiten

De leden van de NSC-fractie vragen hoe de handhaving en naleving van de TFR-verordening geregeld gaat worden. Kan de regering een nadere toelichting geven op de gevolgen van het wetsvoorstel voor de toezichtcapaciteit van De Nederlandsche Bank (DNB) en de Autoriteit Financiële Markten (AFM)?

TFR is een herziening van de bestaande Wire Transfer Regulation (WTR2). De WTR2 bevatte reeds verplichtingen ten aanzien van het vastleggen en uitwisselen van informatie bij girale geldovermakingen door banken en andere betaaldienstverleners. Deze onderdelen worden niet gewijzigd in TFR en op de naleving van deze verplichtingen wordt dus al toezicht gehouden. De meest materiele wijziging in TFR is dat cryptoactiva en cryptodienstverleners binnen de reikwijdte worden gebracht.

Met de Uitvoeringswet wordt geregeld dat de bevoegdheid voor het toezicht op de naleving van TFR toebedeeld wordt aan De Nederlandsche Bank (DNB) indien het gaat over de verplichtingen voor betalingsdienst-aanbieders die voortvloeien uit de verordening en op de verplichtingen uit de Wwft voor zover het een bank of elektronischgeldinstelling betreft die cryptoactivadiensten aanbiedt. De Autoriteit Financiële Markten (AFM) wordt aangewezen waar het gaat over verplichtingen voor aanbieders van cryptoactivadiensten die voortvloeien uit de verordening en op de verplichtingen uit de Wwft (niet zijnde een bank of elektronischgeldinstelling die cryptoactivadiensten aanbiedt). Het toezicht op de naleving van TFR en eventuele handhavende optreden van DNB of de AFM zal worden ingelijfd in het bestaande Wwft-toezicht van deze toezichthouders, met gebruikmaking van hun bestaande toezicht- en handavingsinstrumentarium, waaronder het doen van onderzoek, het opvragen van informatie en het opleggen van een (bestuurlijke) boete.

Met de komst van TFR worden alle cryptoactivadienstverleners onderworpen aan de bestaande regels ter voorkoming van witwassen en terrorismefinanciering zoals opgenomen in de Wwft. Dit betekent dat er nieuwe kennis en ervaring opgedaan moet worden door toezichthouders en ook ingezet wordt op internationale samenwerking. De cryptoactivamarkt is bovendien een bewegelijke markt, waarbij veel cryptocactivadienstverleners nog geen ervaring hebben met toezicht. Dit samengenomen verwachten de toezichthouders een substantiële groei ten aanzien van de benodigde capaciteit. Voor het toezicht dat de AFM zal gaan uitvoeren op de cryptosector is de inschatting dat voor het jaar 2025 36 FTE nodig zal zijn. Vanaf 2026 is de inschatting dat zij 33 fte (6,4 miljoen) nodig zullen hebben voor het doorlopend toezicht, waarvan 7 fte gereserveerd is voor TFR. DNB heeft in 2023–2024 voor het Wwft-toezicht op de cryptoactivadienstverleners 14 fte (4,1 miljoen) begroot. DNB zal deze capaciteit voor de opvolgende jaren behouden voor het toezicht op zowel TFR en MiCA. Hiervan is 6,4 fte gereserveerd voor het toezicht op de instellingen. Het toezicht in het kader van TFR zal met name zien op het uitwisselen van informatie tussen de initiator en de begunstigden van de crypto-overmakingen. Ook het integriteitstoezicht valt hieronder. De kosten die aan de sector worden doorberekend worden opgenomen in het Besluit bekostiging financieel toezicht 2019.

De leden van de NSC-fractie vragen of de regering voornemens is om de ervaringen met het nieuwe regime en mogelijke veranderingen in toezichtskosten te monitoren en zo ja, op welke manier.

Verschillende onderdelen van TFR worden door de Europese Commissie geëvalueerd. Uiterlijk op 1 juli 2026 brengt de Commissie een verslag uit met een beoordeling van de risico's van overmakingen of overdrachten naar of vanuit zelfgehoste adressen. Op uiterlijk 30 juni 2027 zal de Commissie een verslag indienen over de handhaving van deze verordening. Daarnaast zal mijn ministerie zelf ook de ontwikkelingen op de cryptoactivamarkten blijven volgen. De toezichtkosten zijn voor een belangrijk deel afhankelijk van de hoeveelheid instellingen die een vergunningsaanvraag doet. Wanneer er bijvoorbeeld veel meer of minder vergunningsaanvragen zijn dan in eerste instantie voorzien, kunnen de gealloceerde kosten en toezichtinzet mogelijk te laag of te hoog zijn. Omdat er voor de AFM veel nieuwe taken bijkomen en er veel onzekerheid is over het aantal vergunningaanvragen, is met de AFM medio 2025 een evaluatiemoment afgesproken waar wordt gekeken naar de benodigde toezichtinzet. Daarnaast lichten DNB en de AFM de toezichtkosten toe in hun jaarlijkse begrotingen en verantwoordingen. Ik let bij de beoordeling van deze stukken ook op de toezichtinzet voor TFR, mede in het licht van ontwikkelingen op de cryptomarkten en in het toezicht daarop.

De leden van de NSC-fractie vragen verder of de ATR een advies heeft uitgebracht. Zo ja, hoe luidt dit advies?

Het wetsvoorstel is voor advies voorgelegd aan het Adviescollege toetsing regeldruk (ATR). Het adviescollege heeft het dossier niet geselecteerd voor een formeel advies, omdat er geen grote gevolgen voor de regeldruk zijn.

§ 5. Gegevensbescherming

De leden van de NSC-fractie vragen of de Autoriteit Persoonsgegevens een advies heeft uitgebracht. Zo ja, hoe luidt dit advies?

De voorontwerpen van het wetsvoorstel en de memorie van toelichting zijn conform artikel 36, vierde lid, van de Algemene Verordening Gegevensbescherming (AVG) voor advies voorgelegd aan de Autoriteit Persoonsgegevens (AP). De Autoriteit Persoonsgegevens heeft op 26 september 2023 advies uitgebracht.⁴ Zij heeft daarin aangegeven dat het wetsvoorstel haar geen aanleiding geeft tot het maken van opmerkingen.

§ 6.1. Gevolgen voor het bedrijfsleven

De leden van de NSC-fractie vragen of het klopt dat de TFR-verordening leidt tot een flinke uitbreiding van het toezicht ingevolge de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) op crypto-activa transacties (van twee naar negen categorieën).

De leden van de NSC-fractie merken terecht op dat TFR een flinke uitbreiding is van het toezicht. Het huidige registratiekader voor aanbieders van wisseldiensten en bewaarportemonnees, dat opgenomen is in de Wwft op basis van de herziene vierde anti-witwasrichtlijn, wordt vervangen door een omvattender Europees stelsel voor een bredere groep cryptoactivadienstverleners, waarbij de markttoegang en governance worden gereguleerd middels MiCA en de materiële voorschriften ter voorkoming van witwassen en het financieren van terrorisme worden gereguleerd middels TFR en de implementatie daarvan in de Wwft. Alle categorieën aanbieders van cryptoactivadiensten die worden gereguleerd

⁴ <https://autoriteitpersoonsgegevens.nl/documenten/advies-uitvoeringswet-vo-tfr>.

door MiCA, behalve de aanbieders die advies verlenen over cryptoactiva, worden onder het bereik gebracht van de Wwft.

Welke gevolgen heeft dit voor de toezichtskosten, regeldruk en administratieve lasten? Hoeveel extra fte's zal de AFM moeten inzetten om deze wet te handhaven?

De vraag over de toezichtkosten wordt beantwoord in paragraaf 4.4., evenals de vraag over de hoeveelheid extra fte's bij AFM.

De wijzigingen van TFR hebben veelal directe werking en behoeven geen nadere implementatie, behoudens enkele aanpassingen van verwijzingen in bestaande regelgeving. De regeldrukeffecten van deze bepalingen komen derhalve niet voort uit nationale regelgeving, en daarom worden de effecten voor regeldruk niet in beeld gebracht. TFR wijzigt echter ook de vierde anti-witwasrichtlijn waarvan de nationale implementatie wel regeldrukeffecten in zich draagt. Zo wordt de reikwijdte van de Wwft uitgebreid naar alle cryptoactivadienstverleners (behalve partijen die advies verlenen). Op dit moment vallen enkel de aanbieders van bewaarportemonnees en aanbieders van wisseldiensten tussen virtuele en fiduciaire valuta onder de Wwft en de Sanctiewet 1977. Voor deze partijen geldt dat zij aan een aantal nieuwe verplichtingen uit de Wwft zullen moeten voldoen die regeldruk opleveren. Voor de nieuwe aanbieders van cryptoactivadiensten die onder het bereik van de Wwft en Sanctiewet 1977 komen te vallen, geldt dat zij straks zowel aan voor hen nieuwe verplichtingen uit de Wwft als uit de Sanctiewet 1977 moeten voldoen.

Kan de regering deze vragen ook beantwoorden voor de Uitvoeringswet verordening cryptoactiva (Kamerstuk 36 527)?

Voor het antwoord op deze gestelde vragen in het kader van de Uitvoeringswet verordening cryptoactiva verwijs ik u graag naar paragraaf 2 en 2.6. van de nota naar aanleiding van het verslag Uitvoeringswet verordening cryptoactiva.

Overig

De leden van de PVV-fractie vragen de regering om op de volgende vragen te reflecteren. Ten eerste vragen deze leden met betrekking tot transparantie en privacy hoe de balans tussen effectieve witwasbestrijding en de bescherming van de privacy van betrokkenen wordt gewaarborgd binnen de nieuwe regelgeving.

De verschillende verwerkingen van persoonsgegevens op grond van het onderhavige wetsvoorstel volgen rechtstreeks uit verplichtingen uit de vierde anti-witwasrichtlijn. Bij de totstandkoming van de vierde anti-witwasrichtlijn is overwogen dat het belang van het voorkomen van witwassen en financieren van terrorisme het verwerken van persoonsgegevens rechtvaardigt. Tegelijkertijd dient het verwerken van persoonsgegevens beperkt te blijven tot hetgeen noodzakelijk is voor de naleving van de verplichtingen uit de vierde anti-witwasrichtlijn. Dit is ook uitdrukkelijk overwogen bij de totstandkoming van de vierde anti-witwasrichtlijn en komt terug in artikel 34a van de Wwft. Persoonsgegevens die zijn verzameld in het kader van het cliëntenonderzoek mogen niet verder worden verwerkt voor een doel dat onverenigbaar is met dit nalevingsdoel. In artikel 34a Wwft zijn ook andere waarborgen verankerd ter bescherming van persoonsgegevens van cliënten. Zo dient een instelling een cliënt vooraf te informeren over het verwerken van de persoonsgegevens en gelden er bewaartermijnen en de plicht tot

vernietiging van persoonsgegevens na verstrijking daarvan. Ook is de Algemene Verordening Gegevensbescherming van toepassing wanneer er persoonsgegevens verwerkt worden. De Autoriteit Persoonsgegevens heeft op 26 september 2023 advies uitgebracht over het onderhavige wetsvoorstel. Zij heeft daarin aangegeven dat het wetsvoorstel haar geen aanleiding geeft tot het maken van opmerkingen. Hieruit kan ook worden opgemaakt dat in het onderhavige wetsvoorstel de bescherming van privacy afdoende is gewaarborgd.

Ten aanzien van de internationale vergelijking vragen de leden van de PVV-fractie hoe de striktheid van de Nederlandse implementatie van deze EU-verordening zich verhoudt tot die in andere EU-lidstaten, zoals Duitsland, waar strengere regels zijn opgelegd.

Het onderhavige wetsvoorstel ziet op implementatie van een verordening, wat weinig tot geen nationale beleidsruimte met zich meebrengt. In alle lidstaten, ook in Duitsland, gelden dezelfde inhoudelijke normen. Er waren een aantal lidstaattopties, waaronder een optie om langere bewaartermijnen aan te houden. Hiervan is geen gebruik gemaakt, omdat dit niet nodig werd geacht. Graag verwijs ik naar paragraaf 1 dat uitgebreider ingaat op de lidstaattopties en de keuzes die hierin zijn gemaakt.

De leden van de PVV-fractie vragen met betrekking tot toezicht en handhaving welke specifieke maatregelen er zijn genomen om te zorgen voor effectief toezicht en handhaving van deze regelgeving. En hoe zijn deze maatregelen afgestemd met bestaande structuren binnen de Wet op het financieel toezicht?

Het toezicht op de naleving van TFR en eventuele handhavende optreden van DNB of de AFM zal worden ingelijfd in het bestaande toezicht op de Wet ter voorkoming van witwassen en financieren van terrorisme, en niet het toezicht op de Wet op het financieel toezicht. Hierbij wordt aangesloten bij het bestaande toezicht- en handavingsinstrumentarium, waaronder het doen van onderzoek, het opvragen van informatie en het opleggen van een (bestuurlijke) boete. Graag verwijs ik ook naar paragraaf 4.4.

Voorts vragen de leden van de PVV-fractie ten aanzien van de impact op innovatie of de regering kan aangeven welke overwegingen zijn gemaakt om te zorgen dat de regelgeving innovatie binnen de sector van crypto-activa niet onnodig belemmert.

Het onderhavige wetsvoorstel leidt ertoe dat cryptopartijen gelijke normen dienen na te leven op het gebied van het tegengaan van witwassen en terrorismefinanciering als andere dienstverleners in de financiële sector zoals banken, verzekeraars en vermogensbeheerders. Daarnaast dienen cryptopartijen op basis van TFR informatie toe te voegen over de initiator en de begunstigde bij overdracht van cryptoactiva. Een soortgelijke verplichting geldt ook voor betaaldienstverleners als het gaat om girale geldovermakingen. Kortom, met onderhavige wetsvoorstel worden al bestaande normen ook opgelegd aan cryptopartijen. Deze verplichtingen zijn minimaal nodig om een integere financiële sector te waarborgen. De nieuwe eisen zullen ertoe leiden dat aanbieders van cryptodienstverleners meer informatie zullen moeten verzamelen en analyseren, wat zal zorgen voor meer werk aan de kant van deze partijen. Dit hoeft innovatie echter niet in de weg te liggen – voor innovatie is het immers ook belangrijk dat men vertrouwen heeft in de sector, en daar draagt deze regelgeving aan bij.

Ten aanzien van de risico's en veiligheid vragen de leden van de PVV-fractie welke stappen zijn ondernomen om de consumenten en investeerders te beschermen tegen de volatiliteit en de veiligheidsrisico's die gepaard gaan met cryptoactiva.

Onderhavig wetsvoorstel bevat enkel de maatregelen die gelden voor cryptoactivadienstverleners voor het tegengaan van witwassen en terrorismefinanciering, alle overige regels die gelden voor aanbieders van cryptoactiva en cryptoactivadienstverleners zijn vastgelegd in MiCA. Zo bevat MiCA regels over het informeren van consumenten over de aard van de cryptoactiva en risico's die hiermee gepaard gaan en regels die erop toezien dat bij (bepaalde) cryptoactiva de volledige inleg ten alle tijden teruggevorderd kan worden door de consument. Graag verwijs ik de PVV-fractie naar de Uitvoeringswet verordening cryptoactiva voor deze regels.

Op het gebied van internationale samenwerking vragen de leden van de PVV-fractie op welke manier samengewerkt wordt met internationale partners om de regelgeving rondom cryptoactiva te harmoniseren, gezien het internationale karakter van deze markten.

Nederland neemt actief deel aan de Financial Action Task Force. In dit verband wordt internationaal nagedacht over maatregelen om witwassen en terrorismefinanciering tegen te gaan, ook met betrekking tot cryptoactiva. De regels die voortvloeien uit TFR zijn dan ook gestoeld op de FATF-standaarden en sluiten daarmee aan op het internationaal afgesproken standaarden waar ook landen buiten de EU zich aan hebben gecommitteerd. Daarnaast wordt in IMF, G20 en FSB verband de ontwikkelingen in cryptomarkten gemonitord waarbij en ook gesproken over de (stabiliteits)risico's, toezicht, en de regulering van cryptoactiva in verscheidene jurisdicties. Nederland draagt ook in deze samenwerkingsverbanden actief bij aan deze discussies, juist gezien de internationale aard van cryptoactivamarkten.

De leden van de PVV-fractie vragen voorts in het kader van evaluatie en aanpassing hoe de regering de effectiviteit van deze wetgeving zal evalueren. En welke mechanismen zijn ingebouwd om de wetgeving indien nodig aan te passen aan snel veranderende technologische ontwikkelingen?

Voor het antwoord op de vraag van de PVV-fractie over hoe de regering de effectiviteit van de wetgeving zal evalueren, verwijs ik graag naar paragraaf 4.4. waar door de NSC-fractie een vraag van soortgelijke strekking is gesteld.

TFR verwijst naar MiCA voor haar toepassingsbereik. Zodra de reikwijdte van MiCA uitbreidt, zal TFR automatisch van toepassing worden op nieuwe partijen. Dit omdat TFR rechtstreekse werking kent. Daarbij is MiCA zo technisch neutraal mogelijk ingestoken en is geprobeerd rekening te houden met snel veranderende technologische ontwikkelingen bij het opstellen van definities.

Ook vragen de leden van de PVV-fractie wat de verwachte impact van deze regelgeving op de Nederlandse financiële markten en de bredere economie is.

Voor de financiële markten geldt dat er meer gereguleerde partijen bijkomen die kosten zullen maken i.v.m. naleving van de regels. Er wordt geen significante impact verwacht op de bredere economie, anders dan dat er meer criminele geldstromen onderschept en gestopt zullen worden.

Daarnaast leidt het tot meer en betere informatie die cryptodienstverleners kunnen gebruiken om effectief en efficiënt te voldoen aan de eisen van hun poortwachtersfunctie. De informatie kan daarnaast ook door opsporingsdiensten gebruikt worden om criminele transacties op te sporen. Daarnaast zijn er derde partij dienstverleners die technische oplossingen voor het onderling uitwisselen van informatie ontwikkelen.

Tot slot vragen de leden van de PVV-fractie welke specifieke maatregelen in de wetgeving zijn opgenomen om bijvoorbeeld marktmanipulatie te voorkomen.

MiCA bevat een verbod op marktmanipulatie. Om marktmanipulatie te voorkomen moet iedereen die beroepshalve transacties in cryptoactiva tot stand brengt of uitvoert, beschikken over systemen en procedures voor de preventie en opsporing van marktmisbruik. Zo is er een meldingsplicht wanneer er een vermoeden is van marktmanipulatie. Graag verwijs ik de PVV-fractie naar de Uitvoeringswet verordening cryptoactiva voor deze regels.

De Minister van Financiën,
E. Heinen