

Feedbackstatement Q&A van 16 september 2022 over sanctiescreening bij (inkomende en uitgaande) cryptotransacties.

DNB heeft 7 reacties ontvangen. DNB waardeert de ontvangen reacties. Op basis van de reacties is de Q&A op een aantal onderdelen aangepast. In dit feedbackstatement wordt ingegaan op de belangrijkste onderwerpen uit de reacties in de consultatie. Onder wijziging wordt aangegeven of de consultatiereactie aanleiding tot wijziging heeft gegeven.

#	Onderwerp	Details	Reactie DNB	Wijziging
1	Noodzaak verduidelijking naleving sanctie-regelgeving ¹	Uit de reacties bleek dat verduidelijking gewenst is over het nut en de noodzaak van deze nadere uitleg door DNB. In de EU is een aantal verordeningen van toepassing die zien op de bevrozing van economische middelen of tegoeden van gesanctioneerde entiteiten en (rechts)personen. Het niet nakomen van dergelijke bindende bepalingen is strafbaar. Dat geldt dus ook voor een aanbieder van cryptodiensten die bewust of onbewust bijdraagt aan een transactie waar een gesanctioneerde bij betrokken is. DNB is niet belast met de vraag of jegens instellingen handhavend opgetreden moet worden nádat zij betrokken zijn bij een transactie met een gesanctioneerde. DNB is belast met het toezicht op de wijze waarop instellingen (beogen te) voorkomen dat zij een transactie verwerken waar een gesanctioneerde rechtstreeks of onrechtstreeks bij betrokken is. In het bijzonder de effectiviteit van maatregelen die instellingen, waaronder aanbieders van	DNB heeft de verplichtingen die moeten voorkomen dat instellingen bijdragen aan een transactie waar een gesanctioneerde bij betrokken is, uiteengezet in de Regeling toezicht Sanctiewet 1977. DNB beperkt zich tot het beoordelen van de getroffen AO/IC-maatregelen ter uitvoering van de Sanctiewet 1977 (hierna: de Sanctiewet) en de Regeling toezicht Sanctiewet 1977 (hierna: RtSw) vanuit een <i>principle based</i> -benadering. Indien DNB de getroffen maatregelen ontoereikend acht, zal zij de voorschriften handhaven door middel van de haar toegekende handhavingsinstrumenten (bijvoorbeeld een aanwijzing, een boete of last onder dwangsom). De Q&A dient ertoe nadere uitleg te geven om zodoende partijen te helpen en meer duidelijkheid te verstrekken over de verwachtingen van DNB omtrent naleving van relevante bepalingen.	Nee

¹ In dit document wordt de term 'sanctieregelgeving' gebruikt. Hiermee wordt bedoeld op het gehele nationale en internationale kader voor sanctieregelgeving, waaronder dus relevante EU-verordeningen, de Sanctiewet 1977 en de Rtsw.

		cryptodiensten, moeten inrichten om te kunnen voldoen aan de vereisten die voortvloeien uit de Sanctiewet 1977 en daarmee dus de eisen die voortvloeien uit de bovenliggende EU-sanctieverordeningen.		
2	Het begrip 'relatie' wordt door DNB ruim geïnterpreteerd.	Uit de ontvangen consultatiereacties op de concept-Q&A maakt DNB op dat ten aanzien van een aantal concrete situaties onduidelijkheid bestaat over de vraag of (rechts)personen en entiteiten dienen te worden aangemerkt als 'relaties' van de aanbieder van cryptodiensten. Zo bestaat onduidelijkheid ten aanzien van de vraag of de houder van een extern (hosted of unhosted) cryptoadres dient te worden aangemerkt als een relatie. Ook houders van een extern (hosted of unhosted) cryptoadres die betrokken zijn bij een transactie, hetzij als begunstigde van de transactie, worden aangemerkt als een relatie van de aanbieder van cryptodiensten. De aanbieder van cryptodiensten stelt immers bij een uitgaande transactie tegoeden beschikbaar aan de houder van een extern (hosted of unhosted) cryptoadres. Bij een inkomende transactie afkomstig van een extern (hosted of unhosted) cryptoadres dient de aanbieder van cryptodiensten te kunnen bepalen of de tegoeden afkomstig zijn van een gesanctioneerde, teneinde vast te kunnen stellen of de tegoeden bevroren moeten worden	De doelstellingen van de (Europese) sanctiewet- en regelgeving zijn ruim, te weten dat enerzijds geen tegoeden of economische middelen, <u>rechtstreeks</u> of <u>onrechtstreeks</u>, ter beschikking worden gesteld aan (rechts)personen of entiteiten, genoemd in de sanctiewet- en regelgeving, en anderzijds dat alle tegoeden en economische middelen die <u>toebehoren aan, eigendom zijn, in het bezit zijn</u> of <u>onder zeggenschap staan</u> van (rechts)personen of entiteiten, genoemd in de sanctiewet- en regelgeving, dienen te worden bevroren. De Sanctiewet is opgesteld ter uitvoering van (onder meer) Europese sanctieregelgeving. Op basis van de Sanctiewet is aan DNB de taak gegeven er op toe te zien dat ondernemingen hun AO/IC dusdanig inrichten dat zij kunnen voldoen aan de genoemde ruime doelstellingen van de (Europese) sanctieregelgeving. Om deze taak uit te kunnen voeren, is het 'relatie' begrip geïntroduceerd in de RtSw. Het begrip 'relatie', zoals genoemd in de RtSw, dient dan ook te worden uitgelegd aan de hand van de benoemde ruime doelstellingen van (Europese) sanctieregelgeving. Tot de relaties van een aanbieder van cryptodiensten die betrokken zijn bij een inkomende en/of uitgaande cryptotransactie, behoren in ieder geval de cliënten van een aanbieder van cryptodiensten, de uiteindelijk belanghebbenden van de cliënten, de wederpartij bij een cryptotransactie en de begunstigde(n) van een transactie. Deze relaties beschikken immers (op enig moment) rechtstreeks dan wel onrechtstreeks over de tegoeden die de aanbieder van cryptodiensten beschikbaar stelt. De aanbieder van cryptodiensten dient te beoordelen of er ook andere partijen betrokken zijn bij de transactie, waaraan de tegoeden	Ja

		en of een hit moet worden gemeld bij DNB.	rechtstreeks of onrechtstreeks ter beschikking worden gesteld. Ook deze partijen worden aangemerkt als relaties van de aanbieder van cryptodiensten.	
3	Verificatie	In de ontvangen consultatiereacties wordt opgemerkt dat de regelgeving geen verplichting geeft om de identiteit van een relatie te controleren of te verifiëren. Ook is gewezen op disproportionele gevolgen die een verificatie-eis kan hebben voor deze sector en met name kleinere instellingen die daarin actief zijn.	Aanbieders van cryptodiensten dienen op diverse momenten, waaronder bij iedere uitgaande en inkomende transactie, de relaties te screenen tegen de sanctieregelgeving, teneinde vast te kunnen stellen dat geen tegoeden beschikbaar worden gesteld aan gesanctioneerde (rechts)personen of entiteiten, en om te kunnen bepalen of tegoeden moeten worden bevroren omdat deze afkomstig zijn van een gesanctioneerde. Het screenen van relaties kan niet risicogebaseerd worden uitgevoerd. Op het moment dat een aanbieder van cryptodiensten een relatie namelijk niet screent, is er geen mogelijkheid voor de aanbieder van cryptodiensten om zich ervan te vergewissen of de relatie gesanctioneerd is. Indien het risico bestaat dat de opgegeven identiteit niet klopt, zal de aanbieder de identiteit van de bij de cryptotransactie betrokken (rechts)persoon of entiteit met zekerheid moeten vaststellen. Het gaat er bij screening namelijk niet alleen om dat de door de relatie opgegeven naam langs de sanctielijsten wordt gehaald, de aanbieder van cryptodiensten dient maatregelen te treffen om te kunnen vaststellen of de opgegeven gegevens ook daadwerkelijk kloppen en of de aanbieder van cryptodiensten dus geen transactie verricht met een gesanctioneerde. De maatregelen die de aanbieder van cryptodiensten neemt om de identiteit te vast te stellen, kunnen risicogebaseerd worden ingevuld. Dit betekent dat het aan de aanbieder van cryptodiensten is om een inschatting te maken van het risico dat de aanbieder een transactie verricht waarbij een gesanctioneerde betrokken is en om	Ja

			vervolgens te kunnen beoordelen welke maatregelen adequaat zijn om ervoor te zorgen dat het risico op overtreding wordt gemitigeerd. Hierbij dienen aanbieders van cryptodiensten het hoge risico op overtreding of ontwijking van sanctieregelgeving, dat de aard van cryptodienstverlening met zich brengt, in acht te nemen. Als er geen maatregelen tegenover te zetten zijn om het risico op overtreding van sanctieregelgeving bij een cryptotransactie te mitigeren, als maatregelen teveel inspanning vergen of teveel restrisico met zich brengen, dan wordt het risico door de aanbieder van cryptodiensten niet aangegaan.²	
4	Is er bij inkomende en uitgaande transacties door aanbieders van cryptodiensten altijd sprake van hoog risico?	In de reacties op de consultatie wordt enkele keren verzocht om de passage te nuanceren waarin een voorbeeld wordt gegeven van hoog risico.	Ten aanzien van het aanwijzen van transacties van en naar derden als hoog risico wordt er op gewezen dat het begrip 'derden' verschillende mogelijkheden impliceert: self hosted (non custodian) wallets, custodian wallets bij in de EU geregistreerde dienstverleners, custodian wallets bij buiten de EU geregistreerde dienstverleners en custodian wallets bij niet-geregistreerde dienstverleners. De risico's zouden per geval kunnen verschillen. Voorts zouden – zoals DNB eerder opmerkt – alle relevante factoren moeten worden meegenomen in de finale (netto)kwalificatie van het risico. DNB zal de tekst van de concept-Q&A aanpassen door te wijzen op de algemene (hoge) risico's op omzeiling van sanctieregelgeving bij crypto's, gecombineerd met het gegeven dat doorgaans sprake is van dienstverlening op afstand. DNB wijst erop dat binnen dat hoge risico ook verschillende gradaties zijn te maken van dat bewuste risico. Dit doet zich bijvoorbeeld voor in gevallen waarin een aanbieder van cryptodiensten een transactie naar een 'hosted wallet' van een derde, die wordt aangehouden door een elders in de EU geregistreerde aanbieder, faciliteert, ten behoeve van een eigen client die ook een	Ja

² Zie ook Leidraad Financiële Sanctieregelgeving van het Ministerie van Financiën, p. 10.

			'hosted wallet' aanhoudt bij de aanbieder. Het risico op overtreding van sanctieregelgeving is in dit voorbeeld minder groot ten opzichte van het voorbeeld van een transactie die gefaciliteerd wordt naar een 'unhosted wallet', omdat sprake is van een aantal feitelijke waarborgen die het risico op overtreding minder groot maken. Genoemde waarborgen zijn niet aanwezig bij een transactie met een 'unhosted wallet'. De Q&A komt op dit punt te luiden: "De aard van cryptodienstverlening brengt met zich dat sprake is van een hoog risico, nu de techniek een zekere mate van anonimiteit van de houder van een cryptoadres en transacties kan faciliteren, en er in de regel sprake is van dienstverlening op afstand. Dit betekent dat van aanbieders van cryptodiensten een grotere mate van risicomitigatie wordt verwacht. Aan elke soort cryptotransactie kleven andere risico's. Zo verschilt een cryptotransactie naar een hosted wallet van een cliënt van een andere onder dezelfde voorwaarden geregistreerde aanbieder van cryptodiensten zich qua risico van een cryptotransactie naar een unhosted wallet. Het risico van overtreding van de sanctieregelgeving is hoger bij transacties waarbij uit het (niet door de aanbieder beheerde) cryptoadres niet blijkt aan wie dit cryptoadres toebehoort (zoals unhosted/private wallets). Bij cryptotransacties van of naar derden speelt daarom het risico dat crypto's worden overgemaakt naar, of worden ontvangen van, een (rechts)persoon of entiteit als bedoeld in de sanctieregelgeving. Het is de verantwoordelijkheid van de cryptodienstverlener om een inschatting van dit risico te maken en adequate mitigerende maatregelen te nemen."	
5	Proportionaliteit	In een aantal reacties wordt gesteld dat de Q&A een onevenredige last op de instellingen legt. Enerzijds wijzen zij op de hoge regeldruk in samenhang met de	Omvang van een aanbieder van cryptodiensten is niet zozeer van doorslaggevende betekenis voor de invulling van de maatregelen om aan de sanctieregelgeving te kunnen voldoen. De proportionele invulling	Nee

		omvang van hun organisatie. Anderzijds wordt de aard van de te treffen beheersmaatregelen disproportioneel genoemd.	is de aansluiting van de beheersmaatregelen op de aard en de complexiteit van de activiteiten van een instelling en de daarmee samenhangende risico's. Kenmerken die indicatief kunnen zijn voor de noodzaak voor meer indringende maatregelen zijn de hoge mate van grensoverschrijdende transacties en anonimiteit.	
6	Vergelijking beleidsuitingen andere sectoren	In de consultatiereacties wordt gewezen dat de lijn van DNB afwijkt van bestaande beleidsuitingen voor andere sectoren. Zo wordt bijvoorbeeld in de huidige Q&A voor schadeverzekeraars over hetzelfde onderwerp een andere benadering gekozen.	DNB heeft begrip voor de vragen over andere sectoren, met name omdat in sommige uitingen staat dat de sanctiescreening risicogebaseerd kan plaatsvinden. DNB is van mening dat de sanctiescreening niet risicogebaseerd kan geschieden (uiteindelijk moet de instelling immers doorlopend weten of ze geen diensten aan een gesanctioneerde levert, bijvoorbeeld bij de uitvoering van transacties). Een instelling moet dus i. de identiteit van een relatie vaststellen, en ii. haar relaties screenen op een 'hit'. De instelling mag zelf bepalen op welke wijze zij die controle uitvoert en wat daarvoor nodig is. De instelling kan daar een risicogeorïënteerde invulling aan geven, mits deze invulling onderbouwd en gedocumenteerd is. Dit neemt niet weg dat relaties altijd dienen te worden gescreend. Een risicogebaseerde invulling kan bijvoorbeeld worden gegeven aan: a) De frequentie van de periodieke controle of bestaande relaties op een sanctielijst voorkomen. b) De vaststelling of de relatie ook daadwerkelijk de persoon is ten gunste waarvan een financiële dienst of een financiële transactie wordt verricht. Als de risico's op ontwijking van sanctieregelgeving groter zijn, dan moeten de controle op de identiteit van een relatie en het controleren op een 'hit' ook indringender plaatsvinden. c) De technische wijze waarop screening plaatsvindt. DNB zal de overige uitingen de komende tijd naar ditzelfde uitgangspunt formuleren. DNB moet daarbij zorgdragen voor een uniform speelveld. De Sanctiewet 1977 en	Nee

			RtSW zijn onverminderd van toepassing voor andere sectoren. DNB verduidelijkt de status van relevante uitingen tot die tijd met de volgende toevoeging: "Deze informatie is op enkele onderdelen niet langer actueel en zal worden aangepast. DNB verwijst u naar het relevante nieuwsbericht ". Deze zal bij de beleidsuitingen Q&A Sanctiewet voor schadeverzekeraars, Leidraad Wwft en Sw (versie december 2020) en Sanctiecheck wisselinstellingen worden geplaatst.	
7a	Status Q&A's van DNB	Meerdere vragen werden gesteld over de status van Q&A's en good practices van DNB.	Hiervoor verwijst DNB naar haar leeswijzer Beleidsuitingen: Leeswijzer beleidsuitingen DNB. Met deze Q&A geeft DNB inzicht in haar toezichtpraktijk en in haar interpretatie van relevante open normen. In dit geval dus over de sanctiescreening door aanbieders van cryptodiensten. Met de Q&A en de good practices geeft DNB in haar rol als toezichthouder de sector meer duidelijkheid over de verwachtingen bij de toepassing van de Sanctiewet door de instellingen onder haar toezicht. Q&A's bevatten geen zelfstandige toezichtnormen. Q&A's binden DNB in die zin dat een instelling die conform de Q&A handelt, er in principe op kan vertrouwen dat DNB deze handelwijze passend acht. Als instellingen de relevante wet- of regelgeving toepassen in lijn met een Q&A kan DNB hiervan niet afwijken zonder goede onderbouwing. Een instelling kan er dus op rekenen dat DNB haar toezicht ook in lijn met een Q&A zal vormgeven. Anderzijds is een Q&A niet bindend voor instellingen. Een instelling kan op een andere wijze dan in de Q&A aangegeven wijze aan de relevante wet- of regelgeving voldoen. De instelling moet daarbij wel gemotiveerd aan DNB kunnen aantonen dat aan de wet- of regelgeving wordt voldaan.	Nee
7b	Vragen over de status van Good practices van DNB	Een aantal reacties vraagt om verduidelijking van de	Met de good practices worden voorbeelden gegeven van maatregelen die DNB in de praktijk is tegengekomen, welke instellingen	Ja

		status van good practices. Ook wijzen zij op mogelijke aanscherping en verduidelijking van enkele good practices.	<i>kunnen treffen om de risico's op overtreding van sanctieregelgeving te beheersen. Toegelicht wordt: Afhankelijk van de verschillen in risico's kan voor een meer indringende maatregel gekozen worden of voor een combinatie van maatregelen. Het volledige pakket aan maatregelen sluit aan bij de specifieke risico's van de cliënt en de transactie.</i> Uit de reactie op de consultatie blijkt dat sommige partijen menen dat de status van de good practices en het doel wat DNB hoopt te bereiken door deze te publiceren, verduidelijkt kan worden. De huidige tekst van de Q&A voorziet in een duidelijke disclaimer met betrekking tot de status van de good practices: <i>Good practices bevatten suggesties dan wel aanbevelingen voor onder toezicht staande instellingen. Het betreffen voorbeelden van mogelijke toepassingen die naar het oordeel van DNB goede invulling geven aan de verplichtingen uit wet- en regelgeving. Good practices zijn indicatief van aard en instellingen zijn vrij om een andere toepassing te kiezen, zo lang men anderszins voldoet aan de wet.</i> Nadere uitleg over het gebruik van good practices door DNB staat in de Leeswijzer beleidsuitingen DNB. Voorts zal de tekst van de good practices op specifieke onderdelen worden aangepast: - 'Zeer hoog risicolanden' zal worden gewijzigd in 'landen waar sancties op van toepassing zijn' - 'Externe cryptoadressen' zal worden gewijzigd in 'niet door de aanbieder beheerde cryptoadressen' - 'Blokken van cryptoadressen die gelinkt zijn aan illegale activiteiten en door OFAC (Office of Foreign Assets Control) gesanctioneerde adressen' zal worden gewijzigd in 'blokkeren van cryptoadressen die gelinkt zijn aan gesanctioneerde entiteiten en (rechts)personen'	
--	--	--	---	--

			- 'SIRA' zal worden gewijzigd in 'integriteitsrisicoanalyse die de aanbieder in het kader van naleving van de Wwft moet opstellen' - De tussenkop 'Maatregelen om vast te stellen of de door de cliënt opgegeven tegenpartij en/of begunstigde ook daadwerkelijk de ontvanger of verzender is' zal worden verwijderd, de onderste bullets worden toegevoegd aan de lijst erboven.	
8	Samenhang Algemene Verordening Gegevensbescherming (AVG).	Uit de ontvangen consultatiereacties op de concept-Q&A merkt DNB op dat meerdere partijen hebben gewezen op de extensieve verwerking van persoonsgegevens die met de naleving van Sanctiewet en - regelgeving gepaard gaat.	De AVG is van toepassing bij verwerking van persoonsgegevens door aanbieders van cryptodiensten in de rol van poortwachter. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de AVG.	Nee