nederlandse
vereniging
van banken

NVB Sector Standaard

Cryptodienst-verleners

sterke banken
sterke samenleving

Context

Inleiding

Cryptodienstverleners zijn poortwachters van het financiële systeem. Cryptodienstverleners die in Nederland actief zijn, moeten zich registeren bij DNB en zich houden aan de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) en de Sanctiewet. Cryptodienstverleners actief in de EU moeten zich daarnaast houden aan de herziene 4AMLD, de EU-Verordening (2015/847) 'betreffende bij geldovermaking te voegen informatie' en per eind 2024 aan de Markets in Crypto-assets Regulation (MiCaR). Deze NVB Sector Standaard beschrijft de risicogebaseerde aanpak voor banken binnen het huidige regelgevende kader. Dit document wordt, indien nodig, herzien wanneer nieuwe wetgeving wordt geïmplementeerd.

In de Wwft worden de verantwoordelijkheden en de wettelijke verplichtingen van poortwachters beschreven om misbruik van het financiële systeem voor witwassen en terrorismefinanciering te voorkomen. Op hoofdlijnen omvatten deze het klantonderzoek, voortdurende controle en het melden van ongebruikelijke transacties. Cryptodienstverleners zijn verplicht tot het uitvoeren van dezelfde beheersmaatregelen als financiële instellingen.

Dankzij crypto-assets kunnen transacties goedkoper, sneller en makkelijker plaatsvinden. Daarnaast geven crypto-assets mensen die geen toegang hebben tot de traditionele financiële dienstverlening de mogelijkheid om betalingen te doen en te beleggen. Crypto-assets worden steeds meer gebruikt voor transacties en beleggingen, doorgaans voor legitieme doeleinden. Internationaal erkende bronnen wijzen op hoger risico op witwassen en terrorismefinanciering in de cryptosector. Waarbij zij het risico van crimineel misbruik van crypto-assets noemen, evenals het gebruiken van crypto-assets om sancties te omzeilen. De cryptosector biedt dankzij verschillende kenmerken, met name in specifieke segmenten en bij specifieke diensten, een aantrekkelijke mogelijkheid om criminele terroristische geldstromen in het financiële systeem te brengen. Vooral dankzij de anonimiteit, het wereldwijde bereik en de snelheid van de transacties, plus de internationale aard die gepaard gaat met virtuele activa. Criminelen kunnen ook hiaten in de kaders die zijn opgesteld voor het voorkomen van witwassen en terrorismefinanciering benutten door hun illegaal verkregen middelen te verplaatsen naar cryptodienstverleners die gevestigd of actief zijn in jurisdicties waar geen of minimale wetgeving is met betrekking tot witwassen en terrorismefinanciering.

Wanneer een zakelijke relatie of transactie een hoger risico op witwassen of terrorismefinanciering met zich meebrengt, vereist artikel 8 lid 1 van de Wwft van banken dat zij verdiepend klantonderzoek (*enhanced due dilligence* – EDD) uitvoeren. De uitvoering van deze EDD-maatregelen kan impact hebben op de klant, bijvoorbeeld doordat er met regelmaat en herhaaldelijk informatie- en documentatieverzoeken richting de klant worden gedaan. Wanneer het klantonderzoek (*client due diligence* - CDD) niet kan worden afgerond, of mogelijke risico's op witwassen of terrorismefinanciering niet voldoende kunnen worden uitgesloten, kan dit leiden tot beperkte toegang tot financiële diensten, geblokkeerde rekeningen of mogelijk zelfs het afscheid nemen van een klant.

Het is dan ook van het grootste belang dat de risicobeoordeling van de klant proportioneel wordt uitgevoerd ten opzichte van de geïdentificeerde risico's en dat er rekening wordt gehouden met de specifieke omstandigheden van de zakelijke relatie of de transactie. Het hanteren van een risicogebaseerde aanpak stelt banken in staat de mate en diepgang van hun klantonderzoek aan te passen aan de betreffende risico's. Aanvullende informatie- of bewijsstukken hoeven vervolgens alleen te worden opgevraagd wanneer deze de potentiële risico's kunnen verlagen. Hiermee kan een effectief evenwicht worden bereikt tussen het

beheersen en verlagen van de risico's op witwassen en financieren van terrorisme en het borgen van toegang tot het betalingsverkeer.

Om te zorgen voor een proportionele en risicogebaseerde aanpak, dienen banken onderscheid te maken tussen risico's die verband houden met cryptodienstverleners in het algemeen en de risico's van een individuele cryptodienstverlener. Voor het klantonderzoek is het noodzakelijk de risico's van een individuele cryptodienstverlener te beoordelen, inclusief de diensten die deze aanbieder levert.

In dit kader is het van belang op te merken dat er verschillende soorten cryptodienstverleners zijn, die bijvoorbeeld de volgende diensten leveren:

- diensten voor het wisselen tussen crypto-assets en fiat valuta;
- het aanbieden van bewaarwallets om crypto-assets op te slaan

De risico's verschillen per cryptodienstverlener en zijn afhankelijk van de diensten die worden aangeboden.

In het algemeen houden cryptodienstverleners twee soorten rekeningen aan bij de bank:

1 rekeningen voor hun operationele kosten, zoals het betalen van de huur, salarissen, enz.;
2 klantrekeningen die worden gebruikt om fiat valuta te ontvangen van en over te maken naar de klanten van de cryptodienstverlener. Dit kan ook de Stichting Derdengelden-rekening van de cryptodienstverlener zijn die wordt gebruikt voor het bewaren van de gelden van klanten.

Daarnaast zullen banken ook zakelijke relaties hebben met klanten van cryptodienstverleners die middelen overmaken naar de rekening van een cryptodienstverlener voor het kopen van crypto-assets of die middelen ontvangen die zijn verkregen uit de verkoop van crypto-assets.

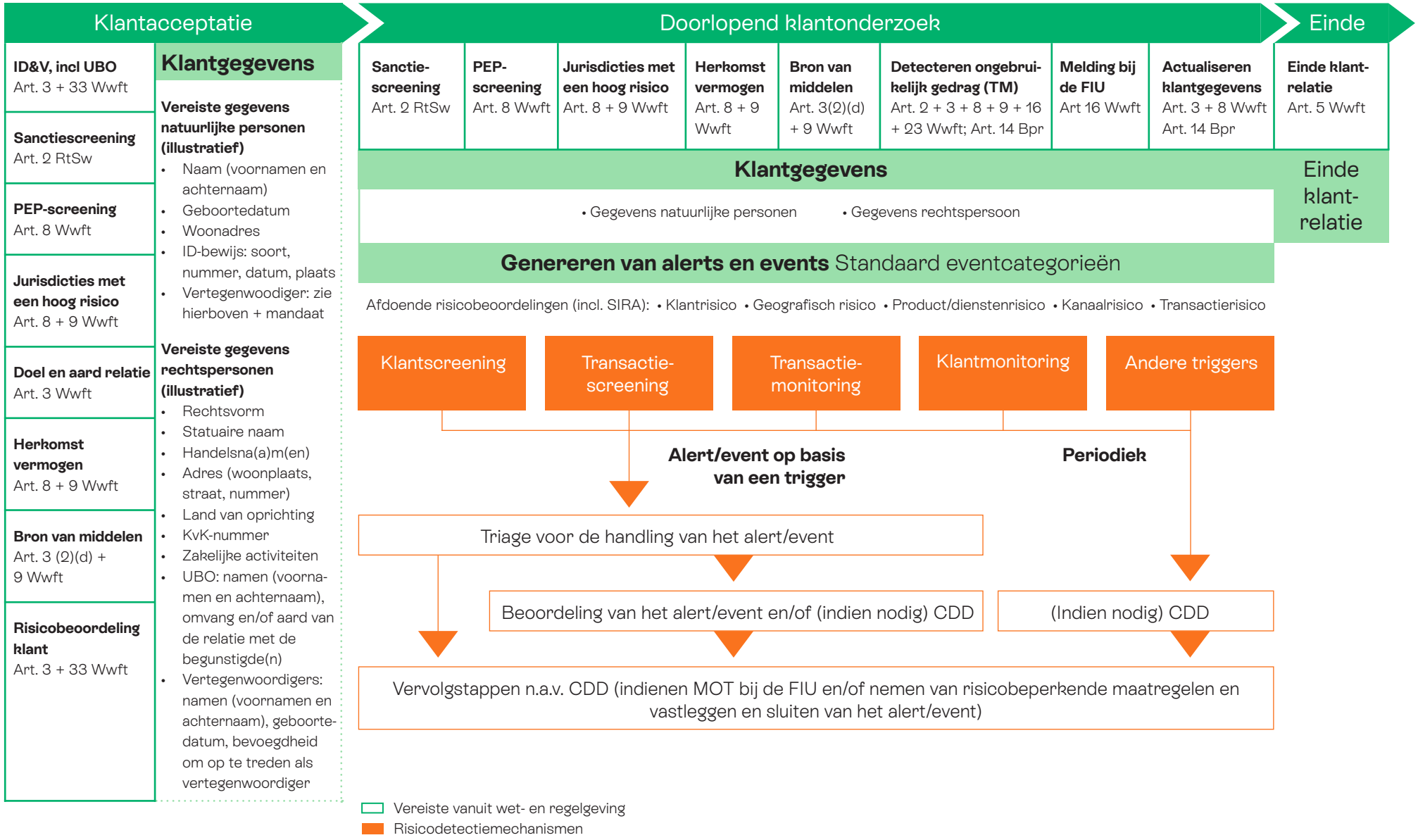
Deze NVB Sector Standaard beschrijft een risicogebaseerde aanpak voor de implementatie van de CDD-vereisten met betrekking tot cryptodienstverleners (dus niet voor hun klanten). Hierbij dienen de risicofactoren per individuele case te worden beoordeeld binnen de volledige context van de klant en de geleverde diensten. Op basis van het uitgevoerde klantonderzoek en de risicobereidheid van de bank besluit de bank per individuele klant of zij een zakelijke relatie met die klant willen aangaan of voortzetten.

De positionering binnen het Financial Crime Framework

De risicobeoordeling van een cryptodienstverlener is onderdeel van het CDD-proces. Alleen wanneer een zakelijke relatie of een transactie hogere risico's op witwassen of terrorismefinanciering met zich meebrengt, zijn EDD-maatregelen nodig om deze risico's bij de individuele klant te verlagen.

Financial Crime Framework

Risicogebaseerd



NVB Standaard

1 NVB Standaard

Voor zowel de banken als voor cryptodienstverleners is het belangrijk dat risico's adequaat worden beoordeeld en indien nodig beperkt. Voor beide partijen is risicobewustzijn een goed uitgangspunt voor een proportionele risicogebaseerde aanpak. Wanneer er een risico wordt vastgesteld, moeten de maatregelen gericht zijn op dat specifieke risico, rekening houdend met het doel van de wetgeving en in context van de sector.

Artikel 8 van de Wwft vereist van banken dat zij EDD uitvoeren wanneer een transactie of een zakelijke relatie een hoger risico op witwassen of terrorismefinanciering met zich meebrengt. Bij de beoordeling van de risico's van een (toekomstige) klant die een cryptodienstverlener is, moet de bank zorgen dat zij voldoende inzicht krijgt in het doel en de aard van de zakelijke activiteiten van de cryptodienstverlener, of de leverancier is geregistreerd of een vergunning heeft in een lidstaat van de EU of de EER of in een ander land met adequate wet- en regelgeving op het gebied van witwassen en terrorismefinanciering, en de mate waarin de cryptodienstverlener zelf CDD-maatregelen toepast.

Risicofactoren	Risicoverlagend	Risicoverhogend
Vergunning of registratie	• Vergunning in de EU of in een derde land	• Geen registratie bij DNB (een DNB-registratie is verplicht wanneer de cryptodienstverlener actief is in NL) • Geen vergunning in de EU of in een derde land
Locatie	• Gevestigd in de EU of in een land met een adequaat regelgevend AML/CFT-kader voor dienstverleners	• Gevestigd in een derde land zonder een adequaat regelgevend AML/CFT-kader
Governance	• UBO's wonen in de EU • Het AML/CFT-beleid en de procedures zijn in lijn met EBA- en DNB-regelgeving • Onafhankelijke compliance- en auditfunctie passend bij de omvang en aard van de organisatie • Een onafhankelijke externe audit	• UBO's wonen niet in de EU • Afwezigheid van AML/CFT-beleid en procedures • Geen compliance- of auditfunctie • Geen onafhankelijk auditrapport door een externe partij beschikbaar • DNB-bevindingen met betrekking tot AML/CFT • Complexe structuur en/of de betrokkenheid van landen met een hoog risico (bijvoorbeeld ten aanzien van transparantie)
Reputatie	• Positief trackrecord • Geen relevante adverse media gerelateerd aan financieel-economische criminaliteit	• Gelinkt aan criminele activiteiten, met name gerelateerd aan witwassen of terrorismefinanciering of andere financieel-economische criminaliteit
Jurisdicties	• Voornamelijk klanten in de EU	• Klanten uit landen met tekortkomingen in het AML/CFT-regime
Transacties en diensten	• Contante stortingen worden niet geaccepteerd • Privacycoins (zoals Monero, Zcash, enz.) mogen niet worden gebruikt voor transacties (bijvoorbeeld het kopen, overboeken, verkopen, stallen of opnemen van middelen) • Alleen wisselen en/of omzetten van crypto naar fiat valuta en andersom (on- en off-ramping) • Alleen walletdiensten • Gebruik van blockchain-analyse om potentieel criminele partijen en patronen te identificeren • Crypto-assets in een bewaarwallets • Voortdurende monitoring van klanten en transacties op AML/CFT en sancties • Closed-loop diensten	• Contante stortingen zijn mogelijk • Privacycoins (zoals Monero, Zcash, enz.) mogen wel gebruikt worden voor transacties (bijvoorbeeld het kopen, overboeken, verkopen, stallen of opnemen van middelen) • Diensten die betrekking hebben op non-fungible tokens (NFT's), decentralised finance (DeFi) • Geen toepassing blockchain-analyse • Crypto-assets worden overgedragen naar een externe wallet • De diensten omvatten het plaatsen van crypto-assets (bijvoorbeeld Initial Coin Offerings) • Maakt gebruik van anonimiserende technieken (bijvoorbeeld AEC's, mixing en tumbling-diensten, privacywallets)
Voortdurende monitoring	• Er vindt adequate voortdurende monitoring plaats van klanten en transacties op zowel AML/CFT als Sancties • Transactiemonitoring in lijn met sectorstandaarden (zoals de FATF) en recente publicaties • Inzet blockchainanalyse voor transparantie van transacties	• Beperkt of geen zicht op het adequaat voldoen aan vereisten van voortdurende monitoring. • Geen monitoring op het gebruik van anonimiserende technieken (bv. mixing)

1.1 Risicofactoren

In de tabel op de vorige pagina staan de kenmerken en het klantgedrag beschreven die door banken als risicoverlagende of risicoverhogende factoren kunnen worden beschouwd bij de risicobeoordeling van een cryptodienstverlener. Deze informatie is ook bedoeld om cryptodienstverleners meer inzicht te geven in de gehanteerde risicofactoren en draagt bij aan een groter bewustzijn ten behoeve van risicobeperking.

Deze risicoverlagende en risicoverhogende factoren staan niet op zichzelf en moeten worden beoordeeld binnen de volledige context van de klant. De risicoclassificatie kan dan ook niet uitsluitend worden bepaald op basis van de aanwezigheid van een enkele risicofactor. Klanten hebben altijd de mogelijkheid om relevante informatie en documentatie aan te leveren om de context van specifieke kenmerken of gedrag toe te lichten. Het is de verantwoordelijkheid van de klant om de bank tijdig van antwoorden op vragen te voorzien om de relatie voort te zetten.

1.2 Informatie en documentatie

Bij het aangaan van een zakelijke relatie met een cryptodienstverlener dragen de volgende informatie en documentatie bij aan een adequate risicobeoordeling en verantwoording van effectieve risicoverlagende maatregelen. Deze lijst is niet uitputtend.

- Governance- en organisatiestructuur, inclusief UBO's, organogram, toelichting op de structuur, aantal werknemers, beleid, procedures, beheersmaatregelen, compliance- en auditfuncties;
- DNB-registratie;
- Een onafhankelijk auditverslag door een externe partij t.a.v. Wwft-verplichtingen;
- Geografische locatie van de (operationele) activiteiten en klanten;
- Informatie over de klantportefeuille;
- Het verwachte transactiegedrag, waaronder inkomende en uitgaande geldstromen, type transactie, omvang, frequentie, betrokken landen, valuta, tegenpartijen, enz.
- Cryptodienstverleners beschikken vaak over een Stichting Derdengelden ter ondersteuning van hun activiteiten. In tegenstelling tot de cryptodienstverlener wordt de Stichting Derdengelden niet geregistreerd bij DNB, maar moet wel worden meegenomen in de algehele beoordeling van de individuele cryptodienstverlener, samen met het doel waarvoor het bedrijf middelen over deze rekening laat lopen.

1.3 Risicobeoordeling

De eerder opgenomen risicoverlagende en risicoverhogende factoren moeten door de banken in overweging worden genomen tijdens het klantonderzoek van een cryptodienstverlener. Deze risicofactoren dienen te worden beoordeeld in de volledige context van de klant. Op deze manier worden de vastgestelde risico's op witwassen en terrorismefinanciering effectief beperkt en wordt tegelijkertijd de toegang tot het betalingsverkeer geborgd. De risicobeoordeling resulteert in een risicoprofiel van de klant op basis van het geheel van verschillende risicofactoren.

Hieronder volgen een aantal voorbeelden van criteria die meegenomen kunnen worden bij het uitvoeren van het klantonderzoek bij een cryptodienstverlener en het beoordelen van de verkregen informatie.

- Het verkrijgen van inzicht in het bedrijfsmodel, inclusief het soort crypto-assets dat de cryptodienstverlener aanbiedt, de aard van de transacties (bijvoorbeeld handelen, beleggen, minen) en de jurisdicties waar de cryptodienstverlener actief is.
- Het beoordelen van de technische capaciteiten, waaronder de effectiviteit van de transactiemonitoringssystemen van de cryptodienstverlener en de mate waarin het bedrijf in staat is transacties op de blockchain te volgen.
- Het beoordelen van de effectiviteit van de compliance- en auditfuncties, inclusief het AML/CFT-beleid en procedures van de cryptodienstverlener.
- Controleren van de status van de wet- en regelgeving in de jurisdicties waarin de operationele activiteiten plaatsvinden.
- Beoordelen van de ervaring en de reputatie van de UBO's en het hoger leidinggevend personeel. Dit kan een controle van de professionele achtergronden omvatten, of eerdere betrokkenheid in de cryptosector, of mogelijke toezicht of juridische kwesties.

- Het verkrijgen van inzicht in het klantenbestand van de cryptodienstverlener, inclusief de soort, locatie en aard van de transacties.

2 Bankklanten die crypto-assets kopen of verkopen

De banken passen CDD-maatregelen toe die passend zijn bij het risicoprofiel van een individuele klant. Als een klant geld overboekt naar een cryptodienstverlener en er is klantonderzoek uitgevoerd, waaronder (indien nodig) naar de bron van de middelen, dan wordt de overboeking naar een cryptodienstverlener niet gezien als een risicoverhogende factor.

Als een klant geld ontvangt van een cryptodienstverlener waardoor er een risico-indicator wordt getriggerd, dient er wel een beoordeling van de bron van middelen te worden uitgevoerd. De NVB Sector Standaard over de bron van middelen biedt uitgangspunten voor de risicobeoordeling van de bron van middelen van een klant. De klant kan informatie bij de bank aanleveren over de rekening bij de cryptodienstverlener waaruit de oorspronkelijke storting blijkt evenals de transacties die zijn gedaan gedurende de periode waarin de klant in het bezit was van crypto-assets of hierin handelde. De Wwft biedt geen wettelijke grondslag die cryptodienstverleners verplicht informatie over hun klanten aan te leveren bij de bank.

3 Impact

Meestal zal contact met de CASP nodig zijn om de benodigde informatie en documentatie te verkrijgen. Door de focus te leggen op de relevante risicofactoren kan dit informatieverzoek proportioneel worden afgestemd op het niveau van de mogelijke risico's op witwassen en het financieren van terrorisme. Bovendien is een gerichte risicogebaseerde aanpak essentieel om onnodige informatieverzoeken richting de klant te voorkomen en de toegang tot financiële diensten te borgen. Ook het gebruik van informatie die afkomstig is uit openbare bronnen en het analyseren van het klant- en transactiegedrag kan de administratieve last verlagen.

Banken kunnen de risicofactoren die in deze NVB Standaard worden beschreven implementeren via hun beleid, procedures en beheersmaatregelen. Hierdoor kunnen de relevante risico's op witwassen en het financieren van terrorisme effectief worden beheerst en wordt tegelijkertijd geborgd dat het uitvoeren van klantonderzoek niet resulteert in een algehele weigering of beëindiging van zakelijke relaties binnen een volledige klantcategorie.

4 Praktijkvoorbeelden

Let op, de praktijkvoorbeelden die hierna volgen zijn voorbeelden om de praktische toepassing van deze NVB Sector Standaard te illustreren en zijn niet uitputtend.

Een Nederlandse cryptodienstverlener

Voorbeeld

Een Nederlandse cryptodienstverlener staat al meer dan twee jaar geregistreerd bij DNB. Zowel de UBO's als het hoger leidinggevend personeel zijn Nederlands. Er is geen adverse media over financieel-economische criminaliteit ten aanzien van de cryptodienstverlener of de UBO's.

NVB Sector Standaard

- Controleer het DNB-register om de registratie te bevestigen.
- Controleer op de website van de cryptodienstverlener welke diensten worden aangeboden.
- Vraag het AML/CFT-beleid op bij de cryptodienstverlener en beoordeel of dit adequaat is.
- Vraag een kopie van de meest recente AML/CFT-audit op bij de cryptodienstverlener.

Een Europese cryptodienst-verlener

Voorbeeld

Een cryptodienstverlener staat al meer dan een jaar geregistreerd bij DNB. Zowel de UBO's als het hoger leidinggevend personeel wonen in de EER. Het hoofdkantoor van de cryptodienstverlener is gevestigd in de EER. Er is geen adverse media over financieel-economische criminaliteit ten aanzien van de cryptodienstverlener of de UBO's.

NVB Standaard

- Controleer het DNB-register om de registratie te bevestigen.
- Controleer op de website van de crypto-dienstverlener welke diensten worden aangeboden.
- Vraag het AML/CFT-beleid op bij de crypto-dienstverlener en beoordeel of dit adequaat is.
- Vraag een kopie van de meest recente AML/CFT-audit op bij de cryptodienstverlener.
- Beoordeel de AML/CFT-controles en verkrijg inzicht in het klantenbestand van de crypto-dienstverlener door middel van een gesprek met de verantwoordelijke Compliance-officer.

Een internationale cryptodienst-verlener

Voorbeeld

Een cryptodienstverlener staat al meer dan een jaar geregistreerd bij DNB. Zowel de UBO's als het hoger leidinggevend personeel wonen niet in de EER. De cryptodienstverlener is wereldwijd actief.

NVB Standaard

- Controleer het DNB-register om de registratie te bevestigen.
- Controleer op de website van de crypto-dienstverlener welke diensten worden aangeboden.
- Vraag het AML/CFT-beleid op bij de crypto-dienstverlener en beoordeel of dit adequaat is.
- Vraag een kopie van de meest recente AML/CFT-audit op bij de cryptodienstverlener.
- Beoordeel de AML/CFT-controles en verkrijg inzicht in het klantenbestand van de crypto-dienstverlener door middel van een gesprek met de verantwoordelijke Compliance-officer.
- Voer een gesprek met de interne auditafdeling over de effectiviteit van het AML/CFT-controlekader van de cryptodienstverlener.

Een internationale cryptodienst-verlener

Voorbeeld

Een cryptodienstverlener staat minder dan een jaar geregistreerd bij DNB. Zowel de UBO's als het hoger leidinggevend personeel wonen niet in de EER. Er is sprake van relevante bevindingen door de toezichthouder; zo heeft DNB een boete gegeven.

NVB Standaard

- Controleer het DNB-register om de registratie te bevestigen.
- Controleer op de website van de crypto-dienstverlener welke diensten worden aangeboden.
- Vraag het AML/CFT-beleid op bij de crypto-dienstverlener en beoordeel of dit adequaat is.
- Vraag een kopie van de meest recente AML/CFT-audit op bij de cryptodienstverlener.
- Beoordeel de AML/CFT-controles en verkrijg inzicht in het klantenbestand van de crypto-dienstverlener door middel van een gesprek met de verantwoordelijke Compliance-officer.
- Voer een gesprek met de interne auditafdeling over het herstellen van de vastgestelde tekortkomingen.
- Optioneel kan er een werkbezoek plaatsvinden bij de cryptodienstverlener.

Context

Het regelgevend kader

De regelgevende context die van toepassing is op dit onderwerp is te vinden in de relevante delen van de toepasselijke wetten, regelgeving en richtlijnen van verschillende autoriteiten, zoals: de FATF, de EBA, het Ministerie van Financiën en DNB. Hieronder volgt een overzicht van het huidige regelgevende kader met betrekking tot cryptodienstverleners.

- **FATF-definitie**
  "Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:
  i. exchange between virtual assets and fiat currencies;
  ii. exchange between one or more forms of virtual assets;
  iii. transfer of virtual assets;
  iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
  v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset."
- **Aanbeveling 15 van de FATF**
  "To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations."
- **Aanbeveling 16 van de FATF (d.w.z. de reisregel)**
  "Countries should ensure that originating VASPs obtain and hold required and accurate originator information and required beneficiary information on virtual asset transfers".
- **Conceptrichtsnoer voor de gewijzigde EBA-richtsnoeren ML/TF-risicofactoren (EBA/CP/2023/11)**
  "9.20 When entering into a business relationship with a customer who is a provider of services in a crypto-assets ecosystem established in a third country, which is not regulated under the Markets in Crypto-Assets Regulation or under any other relevant EU regulatory framework, banks may be exposed to increased risk of ML/TF. Banks should carry out the ML/TF risk assessment of these customers and, as part of this, banks should also consider the ML/TF risk associated with the specific type of crypto-assets.
- **Verordening betreffende cryptoactivamarkten**
  "cryptodienstverlening": elk van de hierna genoemde diensten en activiteiten die verband houden met een crypto-assets:
  (a) het bewaren en beheren van crypto-assets namens cliënten;
  (b) het exploiteren van een handelsplatform voor crypto-assets;
  (c) het omwisselen van crypto-assets voor geldmiddelen;
  (d) het omwisselen van crypto-assets voor andere cryptoactiva;
  (e) het uitvoeren van orders in crypto-assets namens cliënten;
  (f) het plaatsen van crypto-assets;
  (g) het ontvangen en doorgeven van orders in crypto-assets namens cliënten;
  (h) het verlenen van advies over crypto-assets;
  (i) het verzorgen van portefeuillebeheer voor crypto-assets;
  (j) het verlenen van transactieservices voor crypto-assets namens cliënten;
- **Artikel 8 lid 1 Wwft**
  "Een instelling verricht, in aanvulling op artikel 3, tweede tot en met vierde lid, verscherpt cliëntenonderzoek in ten minste de volgende gevallen:
  a. indien de zakelijke relatie of transactie naar haar aard een hoger risico op witwassen of terrorismefinanciering met zich brengt."

Afstemming tussen de ‘DNB Good Practices’ en de ‘NVB Standaard’

DNB heeft als doel organisaties waarop de bank toezicht houdt inzicht te geven in haar beleidspraktijk door bijvoorbeeld een interpretatie van wettelijke toezichtregels te geven (Q&A), evenals voorbeelden van manieren waarop aan de wettelijke toezichtregels kan worden voldaan (Good Practices). Het is hierbij belangrijk op te merken dat noch de Q&A’s, noch de Good Practices van DNB juridisch bindend zijn. DNB geeft ook informatie over de registratievereisten en het toezicht op cryptodienstverleners[1].

In de NVB Standaard worden de toepassing en de uitvoering van de risicogebaseerde aanpak voor cryptodienstverleners in meer detail beschreven. De Standaard is het resultaat van een intensieve samenwerking tussen de banken en de sector, met als doel de efficiëntie van de regelgevende kaders te vergroten door de risicogebaseerde ruimte binnen de verschillende kaders te gebruiken om bestaande mechanismen te verbeteren. Daarnaast geeft de Sector Standaard meer praktische voorbeelden van risicofactoren en risicoverlagende maatregelen voor verschillende scenario’s.

1 https://www.dnb.nl/en/sector-information/open-book-supervision/open-book-supervision-sectors/crypto-service-providers/registration-of-crypto-service-providers/ https://www.dnb.nl/en/public-register/register-of-crypto-service-providers/?p=1&l=10&rc=V1dGVEFD

Nederlandse Vereniging van Banken
Gustav Mahlerplein 29-35
1082 MS Amsterdam
www.nvb.nl