

Annex - Leidraad Wwft en Sanctiewet

Aandachtspunten voor CASPs

Publicatiedatum: mei 2025

Inhoudsopgave

Inleiding	3
Toepasselijkheid Leidraad	4
Toezicht door de AFM	4
Leeswijzer	4
1. Aandachtspunten Wwft	5
1.1. Risicobeoordeling	5
1.2. Belangrijke risicofactoren t.b.v. de risicobeoordeling	5
1.3. Verscherpt cliëntonderzoek	6
1.4. Transactiemonitoring en melden van ongebruikelijke transacties bij FIU-Nederland	7
2. Aandachtspunten Sanctiewet	9
2.1. Risicobeoordeling en maatregelen	9
2.2. Beleid en procedures	9
2.3. Verificatie bij een zelfgehost adres	10
2.4. Sanctiewetmeldingen	10
3. Aandachtspunten Transfer of Funds Regulation (TFR)	12
3.1. Toepassingsbereik	12
3.2. CASP van de initiator	13
3.3. CASP van de begunstigde en de intermediaire CASP	15
3.4. Overdracht naar of vanuit een zelfgehost adres	16
3.5. Herhaaldelijk nalatige CASPs en meldplicht	17
3.6. Aandachtspunten AVG	19
Bijlage – overzicht relevante wetgeving	20

Inleiding

In juni 2024 heeft de AFM een update van de Leidraad Wwft en Sanctiewet (hierna, 'Leidraad') gepubliceerd. Deze Annex is een aanvulling bij de Leidraad en is bedoeld voor aanbieders van cryptoactivadiensten (crypto-asset service providers, hierna 'CASPs').

Vanaf 30 december 2024 kunnen CASPs die over een vergunning of notificatie beschikken op de Europese markt de volgende cryptoactivadiensten aanbieden.¹

- a) het bewaren en beheren van cryptoactiva namens cliënten;
- b) het exploiteren van een cryptoactivahandelsplatform;
- c) het omwisselen van cryptoactiva voor geldmiddelen;
- d) het omwisselen van cryptoactiva voor andere cryptoactiva;
- e) het uitvoeren van cryptoactivaorders namens cliënten;
- f) het plaatsen van cryptoactiva;
- g) het ontvangen en doorgeven van cryptoactivaorders namens cliënten;
- h) het verlenen van advies over cryptoactiva;
- i) het verzorgen van portefeuillebeheer voor cryptoactiva;
- j) het verlenen van cryptoactivaoverdrachtdiensten namens cliënten.

Cryptoactiva en onderliggende technieken kunnen innovatie in de financiële markten brengen. Door gebruik van innovatieve technologieën kunnen waardes snel wereldwijd worden overgedragen. Dit kan ook veel potentiële voordelen bieden, zoals snellere en goedkopere transacties. Vanwege het pseudo-anonieme karakter en het gemak en de snelheid waarmee waardes overal ter wereld kunnen worden verstuurd, zijn cryptoactiva ook aantrekkelijk voor criminelen. Zonder goede regulering dreigen cryptoactiva ook een veilige haven te worden voor witwassen en terrorismefinanciering.²

CASPs moeten aan specifieke *Anti-Money Laundering and Countering the Financing of Terrorism* (hierna, 'AML/CFT') regels voldoen.³ Zo kwalificeren CASPs vanaf 4 februari 2025 als andere financiële onderneming als gedefinieerd in de Wet ter voorkoming van witwassen en financieren van terrorisme (hierna, 'Wwft').⁴ Naleving van de Wwft door CASPs valt per 4 februari 2025 onder toezicht van de AFM.⁵ Als Wwft-instelling hebben CASPs bepaalde verplichtingen om misbruik van het financiële systeem voor witwassen en terrorismefinanciering te voorkomen.

Op grond van de Sanctiewet 1977 (hierna 'Sanctiewet') en de Regeling toezicht Sanctiewet 1977 moeten CASPs per 4 februari 2025 tevens maatregelen treffen op het gebied van de administratieve organisatie en interne controle (AO/IC), om zo te waarborgen dat de bepalingen van de sanctieregelgeving worden nageleefd.

¹ Artikel 63 en 60 MiCAR.

² FATF, Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing en Europol Spotlight 'Cryptocurrencies: tracing the evolution of criminal finances' en National Risk Assessment Witwassen 2023, (WODC, 3 april 2024) p. 74.

³ Door Verordening (EU) 2023/1113 vallen CASPs onder het bereik van de Anti-witwasrichtlijn (Richtlijn (EU) 2015/849). De Uitvoeringswet TFR geeft uitvoering aan deze Verordening. Relevant voor de naleving van regels ter voorkoming van witwassen en financieren van terrorisme zijn tevens de diverse Richtsnoeren die de Europese Bankenautoriteit (hierna 'EBA') heeft gepubliceerd. Het is raadzaam om kennis hiervan te nemen. In deze Annex worden diverse van deze Richtsnoeren aangehaald.

⁴ Artikel 1a, derde lid sub k en l, Wwft.

⁵ Artikel 38 TFR, artikel 3, tweede lid sub g, van de Vierde anti-witwasrichtlijn (Richtlijn (EU) 2015/849) en artikel 1a, derde lid, sub k en l, Wwft. Voor aanbieders van cryptoactivadiensten die vóór 30 december 2024 beschikten over een DNB-registratie (hierna: 'registranten'), geldt dat zij gebruik mogen maken van het overgangsregime dat geldt tot 30 juni 2025. Gedurende de overgangsperiode houdt de AFM toezicht op de naleving van de Wwft en Sanctiewet door registranten.

In aanvulling op de wettelijke vereisten die volgen uit de Wwft en Sanctiewet, dienen CASPs te voldoen aan de AML/CFT-vereisten die zijn vastgelegd in de ‘Verordening bij overdrachten van bepaalde cryptoactiva te voegen informatie en tot wijziging van de Vierde anti-witwasrichtlijn’ (ook wel *Transfer of Funds Regulation*, hierna ‘TFR’).⁶ Zo moeten CASPs bepaalde transactiegegevens meesturen bij iedere afzonderlijke overdracht van cryptoactiva, ook wel de ‘Travel Rule’ genoemd.⁷ Daarnaast zijn door EBA Reisregelrichtsnoeren gepubliceerd.⁸ In deze Annex volgt een toelichting op de verplichting informatie te voegen bij cryptoactivaoverdrachten.

Toepasselijkheid Leidraad

CASPs zijn onderworpen aan AML/CFT-vereisten zoals bepaald in de Wwft en Sanctiewet. Daarom geldt de huidige Leidraad in beginsel in zijn volledigheid ook voor CASPs als een toelichting op de Wwft en Sanctiewet.

In het kort betekent dit dat de CASPs de Leidraad kunnen gebruiken voor het geven van invulling aan de wettelijke verplichtingen die op grond van de Wwft en Sanctiewet van toepassing zijn, onder meer op het gebied van de risicobeoordeling, het opstellen van beleid en procedures, groepsbeleid, het uitvoeren van cliëntenonderzoek, transactiemonitoring, melden van ongebruikelijke transacties en naleving van de Sanctiewet.

Zoals hiervoor aangegeven, zijn op de CASPs nog aanvullende wettelijke vereisten van toepassing, zoals de verplichtingen die voortvloeien uit de TFR. Deze Annex is bedoeld als aanvullende toelichting op sectorspecifieke aandachtspunten voor CASPs en als toelichting op de specifieke wettelijke AML/CFT verplichtingen die op CASPs van toepassing zijn.⁹ De Leidraad en deze Annex dienen dan ook in samenhang te worden gelezen.

Toezicht door de AFM

De AFM houdt toezicht op de naleving van de Wwft en Sanctiewet op een risicogebaseerde wijze. Zij verzoekt daartoe de onder haar toezicht staande instellingen periodiek de Wwft/Sanctiewet-vragenlijst in te vullen. De AFM zal de CASPs eveneens periodiek een Wwft/Sanctiewet-vragenlijst sturen. De AFM gebruikt de informatie die via deze vragenlijst is aangeleverd om risicoprofielen op te stellen van de instellingen.

De verkregen informatie geeft daarnaast een algemeen beeld van de stand van de markt voor wat betreft de inherente witwas- en terrorismefinancieringsrisico’s en de mate van beheersing van deze risico’s. Daarnaast kan de AFM deze informatie gebruiken bij het maken van keuzes in de toezichtstrategie.

Leeswijzer

Deze Annex bestaat uit drie hoofdstukken:

- Hoofdstuk 1 behandelt de sectorspecifieke aandachtspunten van de Wwft,
- Hoofdstuk 2 behandelt de aandachtspunten met betrekking tot de Sanctiewet, en
- Hoofdstuk 3 geeft toelichting op de verplichtingen die volgen uit de TFR.

⁶ Verordening (EU) 2023/1113.

⁷ Verordening (EU) 2023/1113.

⁸ Richtsnoeren betreffende informatievereisten met betrekking tot geldovermakingen en bepaalde overdrachten van cryptoactiva uit hoofde van Verordening (EU) 2023/1113 (“Reisregelrichtsnoeren”): <https://www.eba.europa.eu/publications-and-media/press-releases/eba-issues-travel-rule-guidance-tackle-money-laundering-and-terrorist-financing-transfers-funds-and>.

⁹ In de Leidraad zijn bijvoorbeeld ook sectorspecifieke aandachtspunten voor beheerders van beleggingsinstellingen, beleggingsondernemingen en financiële dienstverleners opgenomen.

1. Aandachtspunten Wwft

In aanvulling op de in de Leidraad opgenomen handreikingen ten aanzien van de Wwft, brengt de AFM hieronder enkele specifieke punten voor CASPs onder de aandacht.

1.1. Risicobeoordeling

Zoals in de Leidraad ook is benadrukt, is het regelgevend kader voor het beheersen van de risico's op witwassen en terrorismefinanciering risicobaseerd. Van CASPs wordt verwacht dat zij een beoordeling maken van de risico's die van toepassing zijn op hun bedrijfsvoering. Dit betekent dat een robuuste risicobeoordeling – als grondslag voor het inrichten van beleid, procedures en maatregelen – van groot belang is voor het adequaat naleven van de Wwft.¹⁰ De maatregelen die een instelling moet nemen om haar risico's vast te stellen en te beoordelen dienen in verhouding te staan tot de aard en de omvang van de instelling.

De CASP dient haar risicobeoordeling toe te spitsen op de cryptoactivadiensten die zij verleent, waarbij steeds rekening moet worden gehouden met de risicofactoren die verband houden met type cliënt, product, dienst, transactie en leveringskanaal en met landen of geografische gebieden. Zo moet op toegankelijke wijze inzichtelijk worden gemaakt waar de risico's op witwassen en terrorismefinanciering voor deze CASP het grootst zijn en hoe deze worden beheerst.

Bij het formuleren van de risicobeoordeling van de CASP, wordt verwacht dat zij hierin onder andere de meest recente nationale risicobeoordeling (hierna: NRA) betreft.¹¹ De verhoogde risico's hebben tot gevolg dat er van de CASP veel verwacht wordt ten aanzien van haar risicobeoordeling en de risicobeheersende maatregelen. Het is in het bijzonder van belang dat de risicobeoordeling van de CASP zich niet beperkt tot abstracte en algemeen geformuleerde risico's.

1.2. Belangrijke risicofactoren t.b.v. de risicobeoordeling

CASPs dienen bij het formuleren van de risicobeoordeling rekening te houden met specifiek voor hen geldende risicoverhogende factoren, zoals het direct en mondiaal kunnen overdragen van cryptoactiva, geen of beperkte begrenzing van transactievolumes en -waarde, een hoge volatiliteit en een bepaalde mate van anonimiteit. In algemene zin bestaat er een relatief hoog risico op witwassen en terrorismefinanciering bij het verlenen van cryptoactivadiensten.

Op 16 januari 2024 heeft de European Banking Authority (hierna: EBA) aanvullende richtsnoeren voor krediet- en financiële instellingen over risicofactoren voor witwassen en de financiering van terrorisme gepubliceerd, die vanaf 30 december 2024 gelden (hierna, 'Richtsnoeren ML/TF-risicofactoren').¹² Een onderdeel van deze aanvullende richtsnoeren ziet op CASPs.

¹⁰ De verplichting risico's te identificeren en te beoordelen volgt uit artikel 2b Wwft. Hierbij dient in ieder geval rekening te worden gehouden met de risicofactoren die verband houden met het type cliënt, product, dienst, transactie en leveringskanaal en met landen of geografische gebieden.

¹¹ Witwassen via aanbieder van financiële cryptodiensten', zie: "National Risk Assessment (NRA) Witwassen 2023, Wetenschappelijk Onderzoek- en Datacentrum (WODC), Cahier 2024-1 (online raadpleegbaar)". In de meeste recente NRA is terrorismefinanciering als één van grootste terrorismefinancieringsdreigingen geïdentificeerd: 'Financiering via aanbieder van 'cryptodiensten', zie: "NRA Terrorismefinanciering 2023, WODC, Cahier 2024-2 (online raadpleegbaar)".

¹² EBA/GL/2024/01, 16 januari 2024, 'Richtsnoeren tot wijziging van richtsnoeren EBA/GL/2021/02 krachtens artikel 17 en artikel 18, lid 4, van Richtlijn (EU) 2015/849 betreffende cliëntenonderzoek en de factoren die kredietinstellingen en financiële instellingen in overweging dienen te nemen wanneer zij het aan afzonderlijke zakelijke relaties en occasionele transacties verbonden witwasrisico en risico van terrorismefinanciering beoordelen (hierna "de Richtsnoeren ML/TF-risicofactoren" genoemd)': [Guidelines on ML/TF risk factors | European Banking Authority](#).

Enkele risicoverhogende factoren die door EBA zijn opgemerkt zijn (niet limitatief):

- Wanneer in korte tijd veel geld wordt ontvangen en/of opgenomen waarbij het geld afkomstig is uit de verkoop van cryptoactiva;
- Het product legt geen beperkingen op aan het totale volume of de totale waarde van de overdrachten;
- Een onderneming die onlangs is opgericht en grote hoeveelheden transacties verwerkt;
- Gebruik van een IP-adres dat is verbonden aan een *darknet* of software dat een hoge mate van anonimiteit biedt of dat gekoppeld is aan meerdere gebruikers;
- Wanneer niet de nodige cliëntinformatie wordt verstrekt;
- Wanneer meerdere betaalaccounts worden gebruikt voor de financiering van de cryptoactiva-account;
- Bij overdrachten van cryptoactiva zijn jurisdicties betrokken met een hoger ML/TF risico;
- Wanneer gebruik wordt gemaakt van nieuwe technologieën die nog niet volledig zijn getest of die een verhoogd ML/TF risico hebben.

Indien de cliënt bij eerdere overdrachten van cryptoactiva heeft voldaan aan de informatievereisten of het gaat om producten met beperkte of lage transactievolumes en -waarden, kan dit risicoverlagend werken. Een andere risicoverlagende factor is wanneer de aard en het toepassingsgebied van de betalingskanalen of -systemen die door de CASP worden gebruikt, zijn beperkt tot closed-loopsystemen of systemen die bedoeld zijn om microbetalingen of betalingen van overheden aan personen of van personen aan overheden te vergemakkelijken.

De AFM verwijst naar de Richtsnoeren ML/TF-risicofactoren voor een overzicht van risicoverlagende en risicoverhogende factoren. Titel I van deze Richtsnoeren ML/TF-richtsnoeren is van algemene strekking. Titel II is sectorspecifiek. In dat kader is Richtsnoer 21 van belang voor CASPs. De sectorspecifieke richtsnoeren dienen in samenhang met Titel I van de Richtsnoeren ML/TF-risicofactoren te worden gelezen. De risicofactoren houden verband met het type cliënt, product, dienst, transactie en leveringskanaal en met landen of geografische gebieden.

De beoordeling van de risico's op witwassen en financieren van terrorisme ligt ten grondslag aan de ontwikkeling van het beleid, procedures en maatregelen, om de geïdentificeerde risico's te beperken en effectief te beheersen.¹³

1.3. Verscherpt cliëntonderzoek

Indien sprake is van een verhoogd risico op witwassen of financieren van terrorisme, verricht de CASP verscherpt cliëntonderzoek¹⁴ en treft zij aanvullende maatregelen als bedoeld in Richtsnoer 21.12 van de Richtsnoeren ML/TF-risicofactoren. De gevallen waarin verscherpt cliëntonderzoek moet worden uitgevoerd, worden op basis van de risicobeoordeling voorafgaande aan de zakelijke relatie of te verrichten transactie bepaald. Daarnaast moet de CASP in ieder geval rekening houden met de risicofactoren die worden genoemd in bijlage III van de herziene vierde anti-witwasrichtlijn.¹⁵ In het beleid van de CASP legt zij vast in welke gevallen en op welke wijze verscherpt cliëntonderzoek wordt uitgevoerd.

¹³ Artikel 2c, eerste lid, Wwft.

¹⁴ Artikel 8 Wwft en titel I van de Richtsnoeren ML/TF-risicofactoren.

¹⁵ Richtlijn (EU) 2015/849. De geconsolideerde versie is hier te vinden: [EUR-Lex - 02015L0849-20241230 - EN - EUR-Lex](#).

Een situatie waarbij verscherpt cliëntenonderzoek moet worden uitgevoerd is bijvoorbeeld in het geval CASPs een correspondentrelatie aangaan¹⁶ en/of wanneer er overdracht plaatsvindt van cryptoactiva naar of vanuit een zelfgehost adres.¹⁷

Wanneer een overdracht plaatsvindt van cryptoactiva naar of vanuit een zelfgehost adres, gaat dit gepaard met potentieel hoge integriteitsrisico's.¹⁸ Zo is bijvoorbeeld niet altijd duidelijk wie de eigenaar is van het adres. Daarom dienen er bij dienstverlening gerelateerd aan een zelfgehost adres risicobeperkende maatregelen te worden getroffen. In dat kader moeten CASPs analyseren welke risico's er aan de transacties verbonden zijn.

Ingeval de CASP kennis heeft (gekregen) dat de informatie over de initiator of begunstigde die het zelfgehoste adres gebruikt niet klopt of indien de CASP bij overdrachten vanuit of naar een zelfgehost adres te maken krijgt met ongebruikelijke of verdachte transactiepatronen of een verhoogd risico op witwassen en terrorismefinanciering, moet de CASP verscherpte cliëntenonderzoekmaatregelen treffen om de risico's op passende wijze te beheersen.

Hierbij dient het te gaan om één of meer van de volgende beheersmaatregelen¹⁹:

- het nemen van risicogebaseerde maatregelen ter identificatie en ter verificatie van de identiteit van de initiator of de begunstigde van een overdracht naar of vanuit een zelfgehost adres, of van de uiteindelijke begunstigde eigenaar van de initiator of begunstigde, onder meer door een beroep te doen op derde partijen;
- het eisen van aanvullende informatie over de oorsprong en de bestemming van de overgemaakte cryptoactiva;
- het aanscherpen van de permanente monitoring van deze transacties;
- alle andere maatregelen om de risico's op witwassen en terrorismefinanciering evenals het risico op niet-uitvoering en ontduiking van gerichte financiële sancties en van gerichte financiële sancties in verband met de financiering van proliferatie te beperken en te beheersen.

De beheersmaatregelen dienen in verhouding te staan tot de vastgestelde risico's.

Gelet op het internationale karakter van de transacties van CASPs, vragen wij aandacht voor paragraaf 5.8 van de Leidraad ten aanzien van verscherpt cliëntenonderzoek, waar nader wordt ingegaan op zakelijke relaties of transacties met derde landen. In deze paragraaf (en paragraaf 5.1) van de Leidraad wordt ook ingegaan op de onboarding op afstand en de EBA's 'Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849'.

1.4. Transactiemonitoring en melden van ongebruikelijke transacties bij FIU-Nederland

1.4.1. Transactiemonitoring²⁰

CASPs moeten bij het invulling geven aan het vereiste een voortdurende controle uit te oefenen op een zakelijke relatie en de tijdens de duur van deze relatie verrichte transacties²¹ onderscheid maken tussen het monitoren van fiat-transacties en het monitoren van cryptoactiva transacties. In beide gevallen dienen CASPs te beschikken over een transactiemonitoringssysteem. CASPs dienen in hun beleid vast te leggen welke tooling

¹⁶ Zie ook artikel 8, vierde lid, Wwft.

¹⁷ Artikel 8, vijfde lid, Wwft. Zelfgehoste adressen zijn adressen die niet zijn gekoppeld aan een CASP of een niet in de Unie gevestigde entiteit die soortgelijke diensten aanbiedt als een CASP;

¹⁸ Memorie van toelichting bij Uitvoeringswet TFR, pagina 4.

¹⁹ Artikel 8, vijfde lid, Wwft.

²⁰ Met transacties wordt hierna ook bedoeld op overdrachten van cryptoactiva, zoals gedefinieerd in de TFR.

²¹ Artikel 3, tweede lid, sub d, Wwft.

bij de transactiemonitoring wordt gebruikt en welke configuratie de tooling heeft, waaronder welke ‘business rules’ (de vooraf gedefinieerde criteria waartegen de transacties worden getoetst op het eventueel ongebruikelijke karakter) gebruikt worden en waarom deze passend zijn.²²

Bij het monitoren van cryptoactivaoverdrachten dienen CASPs geavanceerde analyse-instrumenten toe te passen om het aan transacties verbonden risico te kunnen beoordelen zodat zij in staat zijn de geschiedenis van transacties te traceren en potentiële verbanden met criminele activiteiten, personen of entiteiten vast te stellen. Dit geldt in het bijzonder (maar niet uitsluitend) voor transacties met zelfgehoste adressen.²³

Blockchaintechnologie stelt CASPs in staat om, door middel van het toepassen van blockchainmonitoring, onderzoek te doen naar herkomst en bestemming van cryptoactiva en zo eventuele risico’s op witwassen en terrorismefinanciering te beoordelen

1.4.2. Melden van ongebruikelijke transacties

Tabel 2 van bijlage I van het Uitvoeringsbesluit Wwft 2018 is aangepast en vermeldt de indicatoren voor het melden van ongebruikelijke transacties aan Financial Intelligence Unit (FIU-Nederland):

Aanbieders van cryptoactivadiensten als bedoeld in artikel 3, eerste lid, onderdeel 16, sub a, b en d tot en met j, van Verordening (EU) 2023/1114 van het Europees Parlement en de Raad van 31 mei 2023	Een transactie waarbij de instelling aanleiding heeft om te veronderstellen dat deze verband kan houden met witwassen en financieren van terrorisme.
Aanbieders van wisseldiensten als bedoeld in artikel 3, eerste lid, onderdeel 16, sub c, van Verordening (EU) 2023/1114 van het Europees Parlement en de Raad van 31 mei 2023	Een transactie waarbij de instelling aanleiding heeft om te veronderstellen dat deze verband kan houden met witwassen en financieren van terrorisme. Een transactie van een bedrag van € 10.000, - of meer waarbij een omwisseling plaatsvindt tussen virtuele valuta en contante fiduciaire valuta.

CASPs dienen ervoor te zorgen dat zij geregistreerd zijn als melder bij de FIU-Nederland, zodat zij kunnen voldoen aan de verplichting om onverwijld ongebruikelijke transacties te melden.²⁴ Zie daarover meer in paragraaf 6.2 van de Leidraad.

Het ontbreken van informatie van de initiator of de begunstigde bij overdrachten van cryptoactiva kan ook reden zijn tot het doen van een melding van een ongebruikelijke transactie bij de FIU-Nederland. In paragraaf 3.5 van deze Annex wordt hier nader op ingegaan.

²² Artikel 2c, eerste en tweede lid, Wwft juncto artikel 3, tweede lid, sub d Wwft.

²³ Artikel 21.13 Richtsnoeren ML/FT-risicofactoren.

²⁴ Artikel 16, eerste lid, Wwft.

2. Aandachtspunten Sanctiewet

In aanvulling op de in de Leidraad opgenomen handreikingen ten aanzien van de Sanctiewet, brengt de AFM hieronder enkele specifieke punten voor CASPs onder de aandacht.

Een CASP dient op grond van artikel 2, eerste lid, Regeling toezicht Sanctiewet 1977 (**RtSw**)²⁵ maatregelen te treffen op het gebied van de administratieve organisatie en interne controle (AO/IC) om zo te waarborgen dat de bepalingen van de sanctieregelgeving na worden geleefd.

2.1. Risicobeoordeling en maatregelen

Van de CASP wordt verwacht dat zij een beoordeling van de risico's op sanctieovertreding en sanctie-omzeiling uitvoert, om op deze wijze robuuste maatregelen ter beheersing van deze risico's te treffen. Hiertoe dient de CASP in ieder geval beleid, procedures en maatregelen in te regelen. Daarbij dient de CASP zich telkens ervan te vergewissen dat het risico minimaal is dat bij een dienst of transactie financiële middelen naar een persoon of entiteit als bedoeld in de sanctieregelgeving gaan.²⁶

De maatregelen die getroffen moeten worden dienen ten minste te zien op het screenen van de relaties van de CASP met personen of entiteiten op de sanctielijsten.²⁷ Hiertoe dienen CASPs doorlopende screening toe te passen, bijvoorbeeld door middel van een geautomatiseerd systeem.

Een ander voorbeeld van een robuuste maatregel is het opnemen van geolocatie-instrumenten en instrumenten die gebruik van proxy IP-diensten herkennen, in de gevallen waar verhoogde blootstelling aan sanctiemaatregelen blijkt uit de risicobeoordeling. Op deze wijze kan de CASP identificeren en voorkomen dat haar relaties uit landen met sanctiemaatregelen afkomstig zijn.²⁸

Andere maatregelen bij verhoogde sanctierisico's kunnen zijn:

- bij het aangaan van zakelijke relaties relevante informatie inwinnen over het type bedrijf van de klant en de landen waar de klant zaken doet;
- informatie over de uiteindelijke begunstigde van de cryptoactiva;
- het opvragen van meer gedetailleerde informatie van de klant over het doel van een overdracht van cryptoactiva.²⁹

2.2. Beleid en procedures

Gewaarborgd moet worden dat de AO/IC van de instelling ook in staat stelt sectorale sancties en de sanctionering van distributed-ledger-adressen³⁰ na te leven.

Van de CASP wordt ook verwacht dat in het beleid, de procedures en de maatregelen wordt uitgewerkt welke maatregelen de CASP treft wanneer bijvoorbeeld een match is vastgesteld met een persoon of entiteit op de sanctielijst. Deze maatregelen moeten de CASP in staat stellen de cryptoactiva van de zakelijke relatie

²⁵ De RtSw is van toepassing op CASPs op grond van artikel 10, tweede lid, onder I, Sanctiewet.

²⁶ Toelichting Regeling Toezicht Sanctiewet 1977, Staatscourant 28 september 2005, nr. 188, pg. 21 (par. 4.3).

²⁷ Artikel 2, tweede lid, RtSw.

²⁸ Guidelines EBA/GL/2024/15. De richtsnoeren zijn aangenomen op 14 november 2024 en zijn van toepassing per 30 december 2025.

²⁹ Guidelines EBA/GL/2024/15. De richtsnoeren zijn aangenomen op 14 november 2024 en zijn van toepassing per 30 december 2025.

³⁰ Zie voor een definitie artikel 3, onder 18, TFR.

onmiddellijk te kunnen bevroren. In dit beleid werkt de CASP ook het relatiebegrip uit. In paragraaf 9.2 van de Leidraad wordt het begrip relatie nader toegelicht.

EBA's Richtsnoeren inzake interne beleidslijnen, procedures en controles ter waarborging van de uitvoering van beperkende maatregelen van de Unie en de lidstaten³¹, die naar verwachting vanaf 30 december 2025 van kracht zullen zijn, geven handvatten bij de inrichting van het beleid omtrent sanctiescreening door de CASP.

Daarnaast volgt uit deze EBA Richtsnoeren dat de CASP bij het uitvoeren van sanctiescreening in ieder geval de volgende data beoordeelt om te bepalen of hierop mogelijk sanctiebeperkingen van toepassing zijn:³²

- Informatie over de initiator en de begunstigde;
- Doel van de overdracht van cryptoactiva en afhankelijk van de mate waarin de instelling aan sanctierisico's wordt blootgesteld, andere data die informatie verschaft over de feitelijke verzender/ontvanger van cryptoactiva;
- Details van CASPs die betrokken zijn bij de overdracht van cryptoactiva, met inbegrip van intermediaire instellingen, correspondenten, met screening van identificatiecodes;
- Andere details van de overdracht van cryptoactiva, afhankelijk van de aard, het type van de transactie, de ontvangen ondersteunende documentatie, indien informatie beschikbaar is en onderworpen aan de beoordeling van de blootstelling aan sanctiemaatregelen;
- Portemonnee-adressen (Engels 'wallet addresses') van de opdrachtgever en de begunstigde van een overdracht van cryptoactiva, voor zover deze informatie beschikbaar is in officiële lijsten van portemonnee-adressen die gekoppeld zijn aan sanctiemaatregelen.

2.3. Verificatie bij een zelfgehost adres

In het geval van een overdracht van cryptoactiva vanuit of naar een zelfgehost adres, bestaat het risico dat het zelfgehost adres in eigendom is of onder zeggenschap staat van een persoon of entiteit als bedoeld in de sanctieregelgeving, in plaats van de cliënt. Indien de CASP van oordeel is dat het risico meer dan minimaal is dat er financiële middelen ter beschikking worden gesteld aan personen of entiteiten als bedoeld in de sanctieregelgeving, dient de CASP de identiteit van de persoon met eigendom of zeggenschap over het zelfgehost adres te verifiëren. Onderdeel van de AO/IC-maatregelen van de CASP die transacties verricht met zelfgehoste adressen moet daarom zijn:

- Een risicobeoordeling inzake wanneer er een meer dan minimaal risico bestaat dat financiële middelen ter beschikking worden gesteld aan personen of entiteiten als bedoeld in de sanctieregelgeving;
- Beleid met betrekking tot in welke situaties de identiteit van de persoon of entiteit met eigendom of zeggenschap over het zelfgehoste adres geverifieerd dient te worden;
- Beleid inzake de inhoud van die verificatiemaatregelen.

2.4. Sanctiewetmeldingen

In 2024 is de Wet internationale sanctiemaatregelen door de Rijksoverheid geconsulteerd.³³ In het wetsvoorstel staat de instelling van een centraal meldpunt voor sanctiemeldingen. Totdat een dergelijk centraal meldpunt voor sanctiemeldingen is ingeregeld, dienen CASPs de meldingen, als bedoeld in artikel 3 RtSw, in te dienen bij de AFM. Dit geldt ook voor registranten die voorheen meldingen deden bij DNB. Het

³¹ Richtsnoeren EBA/GL/2024/15. De richtsnoeren zijn aangenomen op 14 november 2024 en zijn van toepassing per 30 december 2025.

³² Richtsnoer 21 van de EBA Richtsnoeren "Richtsnoeren inzake interne beleidslijnen, procedures en controles ter waarborging van de uitvoering van de beperkende maatregelen van de Unie en de lidstaten (EBA/GL/2024/14)": [Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures | European Banking Authority](#).

³³ <https://www.internetconsultatie.nl/sanctiemaatregelen/b1>.

meldformulier kan gedownload worden van de website van de AFM³⁴ en ingediend worden per e-mail via meldingsanctiewet@afm.nl. Raadpleeg voor de meest up-to-date informatie over het doen van de sanctie-hit-meldingen bij de AFM de website van de AFM.

Voor de verdere vereisten omtrent de inhoud van de vastlegging van beleid en procedures in de AO/IC en de melding aan de AFM in het geval van een 'sanctie-hit' wordt verwezen naar paragraaf 9 van de Leidraad.

³⁴ [Sanctiewet 1977](#)

3. Aandachtspunten Transfer of Funds Regulation (TFR)

De traceerbaarheid van overdrachten van cryptoactiva kan een bijzonder belangrijk en nuttig hulpmiddel zijn om witwassen en terrorismefinanciering te voorkomen, op te sporen en te onderzoeken. De TFR verplicht (intermediaire) CASPs daarom informatie bij overdrachten van cryptoactiva te voegen en controles uit te oefenen op ontvangende overdrachten, zodat informatie over de initiator en de begunstigde in de gehele keten van overdracht van cryptoactiva herleidbaar blijft. Dit wordt ook wel de ‘*Travel Rule*’ of ‘*Reisregel*’ genoemd.³⁵

Voor betalingsdienstaanbieders bestonden in de TFR al verplichtingen om bij geldovermakingen informatie te voegen om de traceerbaarheid te verbeteren ten behoeve van het voorkomen en opsporen van, en het onderzoeken van witwassen en terrorismefinanciering.³⁶ Met de herschikking van de TFR is het toepassingsgebied per 30 december 2024 uitgebreid zodat ook overdrachten van cryptoactiva binnen het toepassingsgebied van de TFR vallen.

3.1. Toepassingsbereik

De TFR is van toepassing op CASPs van de initiator, CASPs van de begunstigde en op intermediaire CASPs. Er moet sprake zijn van een overdracht van cryptoactiva,³⁷ uitgevoerd door ten minste één CASP die in de Europese Unie is gevestigd of daar haar statutaire zetel heeft.

De TFR verstaat onder overdrachten van cryptoactiva het volgende: “een transactie met als doel cryptoactiva van één distributed-ledger-adres, cryptoactivarekening of ander hulpmiddel [AFM: in Engelse tekst wordt de term ‘*device*’ gebruikt] voor de opslag van cryptoactiva naar een ander te verplaatsen, uitgevoerd door ten minste één CASP die optreedt namens een initiator of een begunstigde, ongeacht of de initiator en de begunstigde dezelfde persoon zijn en ongeacht of de CASP van de initiator en die van de begunstigde dezelfde zijn”.³⁸

De TFR geldt niet indien de initiator en begunstigde CASPs zijn die voor eigen rekening handelen of in gevallen waarin personen cryptoactiva overmaken zonder betrokkenheid van een CASP.³⁹ De TFR bevat geen uitzondering voor intra-groep transacties.

CASPs dienen in hun beleid en procedures vast te leggen welke transacties in het kader van haar cryptoactivadienstverlening binnen het toepassingsbereik van TFR vallen. Hieruit moet volgen bij welke transacties de CASP de initiator is en bij welke de begunstigde (zie paragraaf hierna). Indien er transacties in het kader van de cryptoactivadienstverlening van de CASP niet onder het toepassingsbereik van de TFR vallen, dient de CASP weer te geven welke transacties dit betreft en welke uitsluitingen of afwijkingen als bedoeld in artikel 2 TFR dit betreffen.

³⁵ Uit de preambule van de TFR blijkt dat de EU met de TFR invulling geeft aan haar commitment de 40 aanbevelingen van de Financial Action Task Force (FATF) te implementeren, in het bijzonder ten aanzien van aanbeveling 16.

³⁶ Zie Verordening (EU) 2015/847.

³⁷ Met inbegrip van overdrachten van cryptoactiva, die worden uitgevoerd door middel van cryptogeldautomaten.

³⁸ Artikel 1, onderdeel 10, TFR.

³⁹ Zie voor de reikwijdte verder artikel 2 TFR.

3.2. CASP van de initiator

De CASP van de initiator zorgt voor adequate en geverifieerde informatie over de initiator en de begunstigde bij overdrachten van cryptoactiva. Artikel 14 TFR bepaalt dat de CASP informatie dient te verzamelen, te bewaren en te voegen bij de overdracht van cryptoactiva. De CASP van de initiator staat het initiëren of uitvoeren van overdrachten van cryptoactiva niet toe voordat de volledige naleving van artikel 14 TFR is gewaarborgd.⁴⁰

3.2.1. Te voegen informatie over de initiator

Artikel 14, eerste lid, TFR geeft weer welke informatie over de initiator de CASP van de initiator bij de overdracht van cryptoactiva dient te voegen.

In elk geval moet bereikt worden dat de identiteit van de initiator wordt vastgesteld. Daarbij moet ten minste de naam en het adres van de initiator worden gevoegd, inclusief de naam van het land, in combinatie met additionele informatie. Het moet daarbij gaan om een combinatie van de volgende informatie: het nummer van het officiële persoonlijke document en het cliëntidentificatienummer⁴¹ of geboorteplaats en -datum van de initiator, voor zover deze combinatie leidt tot de vaststelling van de identiteit van de initiator.⁴² Het voegen van de geboorteplaats en -datum fungeert als alternatief voor het cliëntidentificatienummer.

Daarnaast moet de CASP van de initiator de volgende informatie voegen bij de overdracht van cryptoactiva:

- Het distributed-ledger-adres van de initiator, indien de overdracht is geregistreerd op een netwerk dat gebruik maakt van distributed ledger-technologie⁴³ (hierna 'DLT') of vergelijkbare technologie, en het cryptoactivarekeningnummer van de initiator indien een dergelijke rekening bestaat en wordt gebruikt om de transactie te verwerken;
- Het cryptoactivarekeningnummer van de initiator, indien de overdracht niet is geregistreerd op een netwerk dat gebruik maakt van DLT of vergelijkbare technologie;
- Op voorwaarde dat het benodigde veld bestaat in het format voor betalingsberichten, en de initiator deze informatie aan zijn CASP heeft verstrekt, de huidige LEI⁴⁴ of, bij gebrek daaraan, een andere beschikbare officiële gelijkwaardige identificatiecode van de initiator.⁴⁵

Overeenkomstig artikel 14, zesde lid, TFR verifieert de CASP van de initiator voor de overmaking van cryptoactiva de juistheid van de in het eerste lid genoemde informatie over de initiator op basis van documenten, gegevens of informatie uit betrouwbare en onafhankelijke bron. In de Leidraad wordt nader ingegaan op betrouwbare en onafhankelijke bronnen.

Het zevende lid van artikel 14 TFR benoemt een uitzonderingsmogelijkheid op de verificatieplicht van artikel 14, zesde lid, TFR. Indien de CASP de identiteit van de initiator heeft geverifieerd op grond van de vereisten van het cliëntenonderzoek die op de CASP van toepassing zijn uit hoofde van de AMLD⁴⁶, wordt geacht dat de verificatie reeds heeft plaatsgevonden en dus niet opnieuw hoeft te worden uitgevoerd.

⁴⁰ Artikel 14, achtste lid, TFR.

⁴¹ Zie voor de definitie van cliëntidentificatienummer de Reisregelrichtsnoeren, p. 58-59: "Following the FATF approach, the customer identification number refers to a number that uniquely identifies the originator to the originating financial institution and is a different number from the unique transaction reference number. The customer identification number must refer to a record held by the originating financial institution which contains at least one of the following: a national identity number, or a date and place of birth.

⁴² Zie ook artikel 35 e.v. van EBA/GL/2024/11, 4 juli 2024, 'Richtsnoeren betreffende informatievereisten met betrekking tot geldovermakingen en bepaalde overdrachten van cryptoactiva uit hoofde van Verordening (EU) 2023/1113' (hierna de 'Reisregelrichtsnoeren' genoemd).

⁴³ Zie voor de definitie artikel 3, onder 24, TFR.

⁴⁴ Legal Entity Identifier, zie voor de definitie artikel 3, onder 23, TFR.

⁴⁵ Richtsnoer 41 van de Reisregelrichtsnoeren.

⁴⁶ Zie artikel 13 en 14, vijfde lid, van Richtlijn (EU) 2015/849.

3.2.2. Te voegen informatie over de begunstigde

Artikel 14, tweede lid, TFR geeft weer welke informatie over de begunstigde de CASP van de initiator bij overdrachten van cryptoactiva dient te voegen:

- De naam van de begunstigde;⁴⁷
- Het distributed-ledger-adres van de begunstigde, indien de overdracht is geregistreerd op een netwerk dat gebruik maakt van DLT of vergelijkbare technologie, en het cryptoactivarekeningnummer van de begunstigde als een dergelijke rekening bestaat en wordt gebruikt om de transactie te verwerken;
- Het cryptoactivarekeningnummer van de begunstigde, indien de overdracht niet is geregistreerd op een netwerk dat gebruik maakt van DLT of vergelijkbare technologie’;
- Op voorwaarde dat het benodigde veld bestaat in het format voor betalingsberichten, en de initiator deze informatie aan zijn CASP heeft verstrekt, de huidige LEI⁴⁸ of, bij gebrek daaraan, een andere beschikbare officiële gelijkwaardige identificatiecode van de begunstigde.⁴⁹

3.2.3. Informatie bij een gezamenlijke rekening/adres/portemonnee

Voor overdrachten vanaf een gezamenlijke rekening, een gezamenlijk adres of een gezamenlijke portemonnee (Engels ‘wallet’) dient de informatie van alle rekening-, adres- of portemonneehouders te worden verstrekt. Indien de doorgifte van de hiervoor benoemde informatie van alle partijen wegens technische beperkingen als bedoeld in artikel 24 van de Reisregelrichtsnoeren niet kan plaatsvinden, dient de CASP van de initiator de informatie te vermelden van de rekening-, adres- of portemonneehouder die opdracht heeft gegeven tot de overmaking/overdracht, of anders van de primaire rekening-, adres- of portemonneehouder.⁵⁰

3.2.4. Informatie bij een blocovermakingen/batch file transfers

In het geval van een blocovermaking (‘batch file transfers’ conform Engelse vertaling) is het mogelijk dat de CASP in één keer alle vereiste gegevens⁵¹ verstrekt. Hierbij moet wel aan de volgende voorwaarden worden voldaan, namelijk: (i) alle transacties dienen in één batchbestand te worden aangeleverd die alle vereiste en geverifieerde informatie bevat, (ii) iedere transactie dient afzonderlijk binnen dit batchbestand een DLT-adres, cryptoactivarekeningnummer of unieke identificatiecode van de overdracht te bevatten en (iii) alle transacties dienen afkomstig te zijn van één initiator. Dit betekent dat, wanneer het batchbestand meerdere initiators bevat, alle informatie afzonderlijk moet worden verstrekt.⁵²

3.2.5. Wanneer en op welke wijze informatie toevoegen?

De eerdergenoemde informatie over de initiator en de begunstigde moet eerder, tegelijkertijd of gelijktijdig (simultaan) met de overdracht worden ingediend, maar hoeft niet rechtstreeks worden gehecht aan of worden opgenomen in de overdracht zelf. De CASP draagt zorg dat het bijvoegen van informatie niet strijdig is met de bepalingen in de Algemene Verordening Gegevensbescherming, hierna: ‘AVG’. Zie paragraaf 3.6 van de Annex inzake de AVG.

⁴⁷ Richtsnoer 35 van de Reisregelrichtsnoeren.

⁴⁸ *Legal Entity Identifier*, zie voor de definitie artikel 3, onder 23, TFR.

⁴⁹ Richtsnoer 41 van de Reisregelrichtsnoeren.

⁵⁰ Richtsnoer 40 van de Reisregelrichtsnoeren.

⁵¹ De gegevens als bedoeld in artikel 14, eerste lid, TFR.

⁵² Artikel 15 TFR.

CASPs dienen voor de verzending en ontvangst van informatie gebruik te maken van infrastructuren en diensten die over de technische capaciteit beschikken om de informatie volledig, zonder hiaten of fouten, te verzenden en ontvangen.⁵³

3.3. CASP van de begunstigde en de intermediaire CASP

3.3.1. Volledigheid en juistheid van de informatie

CASPs van de begunstigde en intermediaire CASPs stellen procedures in om te onderzoeken en te beoordelen of de meegestuurd informatie volledig is.⁵⁴ Voor een overzicht van de te beoordelen of mee te sturen informatie, wordt verwezen naar voorgaande paragraaf. Deze procedures moeten op een risicogebaseerde manier worden uitgevoerd.

3.3.2. Verificatie van de informatie

Voordat cryptoactiva beschikbaar worden gesteld aan de begunstigde verifieert de CASP van de begunstigde de juistheid van de in artikel 14, tweede lid, TFR bedoelde informatie over de begunstigde op basis van documenten, data of informatie uit een betrouwbare en onafhankelijke bron.⁵⁵ In de Leidraad wordt nader ingegaan op betrouwbare en onafhankelijke bronnen. De CASP van de begunstigde en de intermediaire CASP staan het niet toe overdrachten uit te voeren, indien de vereiste informatie ontbreekt of onvolledig is en daardoor niet wordt voldaan aan artikel 16, eerste en tweede lid, TFR.

3.3.3. Uitvoering, weigering, terugzending of opschorting

De CASP dient te beschikken over beleid en procedures, gebaseerd op haar risicobeoordeling en *risk appetite*, inzake de gevolgen die zij verbindt aan de constatering dat informatie onvolledig is. Hierin dient te staan in welke gevallen de overdracht wordt uitgevoerd, geweigerd, teruggezonden of opgeschort.⁵⁶ Een CASP die ontdekt dat vereiste informatie ontbreekt terwijl zij monitoring *in realtime* uitvoert, maar, na overweging van alle relevante risico's, besluit de overdracht van cryptoactiva uit te voeren, legt vast om welke reden zij die overmaking uitvoert. Een CASP kan een overdracht ook weigeren of terugzenden en de reden hiervan aan de andere CASP mededelen. Indien een overdracht wordt opgeschort, stelt de CASP de andere CASP hiervan in kennis en verzoekt om de ontbrekende informatie.

Wanneer de gevraagde informatie niet wordt verstrekt binnen de gestelde termijn(en), moet de CASP beslissen of zij de overdracht weigert of uitvoert en documenteert de CASP dit adequaat.⁵⁷ Indien weigering technisch niet mogelijk is, dienen de overgedragen cryptoactiva aan de initiator te worden teruggezonden. Indien terugzending naar het oorspronkelijke adres niet mogelijk is, dienen CASPs alternatieve methoden toe te passen. Welke alternatieve methode de CASP beoogt toe te passen, dient opgenomen te worden in het beleid en deze moet onder meer inhouden dat de teruggezonden activa op een beveiligde, afgescheiden rekening worden bewaard terwijl met de initiator wordt gecommuniceerd over een geschikte terugzendingsmethode.⁵⁸

⁵³ In afwijking hiervan mogen CASPs tot en met 31 juli 2025 bij wijze van uitzondering gebruikmaken van infrastructuur of diensten met technische beperkingen wat betreft de volledigheid van gegevens, zolang die worden gecompenseerd door aanvullende technische maatregelen of correcties om volledig aan de Reisregelrichtsnoeren te voldoen. Deze aanvullende procedures dienen ten minste alternatieve mechanismen te omvatten voor het verzamelen, bewaren en ter beschikking stellen van de informatie die vanwege technische beperkingen niet kan worden doorgegeven aan de ontvangende CASP in de overdrachtsketen. Zie Richtsnoeren 21 en 24 van de Reisregelrichtsnoeren.

⁵⁴ Artikel 16, eerste lid, en 20, eerste lid, TFR. Bij de CASP van de begunstigde betreft het de informatie van artikel 14, eerste en tweede lid, TFR over de initiator en de begunstigde. Bij de intermediaire CASP betreft het de informatie van artikel 14, eerste lid, punten a, b en c, en tweede lid, punten a, b en c, TFR.

⁵⁵ Artikel 16, derde lid, TFR.

⁵⁶ Artikel 17, eerste lid, TFR.

⁵⁷ Richtsnoer 64 van de Reisregelrichtsnoeren.

⁵⁸ Richtsnoer 55 van de Reisregelrichtsnoeren.

In dit verband wordt verwezen naar paragraaf 3.5 waar wordt ingegaan op herhaaldelijk nalatige CASPs.

3.4. Overdracht naar of vanuit een zelfgehost adres

3.4.1. Vastleggen in beleid

Wanneer cryptoactiva worden overgedragen naar of vanuit een zelfgehost adres, kunnen er in het bijzonder uitdagingen bestaan bij het identificeren van de initiator of de begunstigde. De TFR kent daarom een aantal bijzondere bepalingen die specifiek gelden bij overdracht naar of vanuit een zelfgehost adres. Voor de aanvullende cliëntonderzoeksmaatregelen bij overdrachten naar of vanuit een zelfgehost adres, wordt ook verwezen naar paragraaf 1.3 van deze Annex inzake verscherpt cliëntenonderzoek.

Wanneer er een overdracht plaatsvindt van cryptoactiva naar of vanuit een zelfgehost adres, gaat dit gepaard met potentieel hoge integriteitsrisico's. CASPs dienen het risico dat gepaard gaat met de overdracht van of naar een zelfgehost adres te beoordelen.⁵⁹ De CASP dient dit per geval te beoordelen. Van de CASP wordt verwacht dat zij de risico's op witwassen en terrorismefinanciering door zelfgehoste adressen in kaart brengt en beleid opstelt om deze risico's adequaat en passend te beheersen.

Verwacht wordt dat de CASP beschikt over risicogebaseerde procedures met betrekking tot de wijze van verificatie. In deze procedures legt zij vast welke verificatiemethode(n) zij hanteert. Daarnaast dient de CASP vast te leggen van welke verificatiemethode zij gebruik maakt, indien één verificatiemethode niet afdoende is. De CASP beoordeelt per geval de gekozen verificatiemethode passend is bij de geïdentificeerde integriteitsrisico's van de betreffende cliënt.

3.4.2. Identificatie van zelfgehost adres

Om aan deze bepalingen te kunnen voldoen, dienen CASPs in de eerste plaats te identificeren of er al dan niet sprake is van een overdracht van cryptoactiva vanuit en naar een zelfgehost adres. Hiertoe dient de CASP van de initiator of de CASP van de begunstigde de beschikbare technische middelen te benutten. Hieronder wordt begrepen, maar dit beperkt zich niet tot: blockchainanalyse, externe gegevensaanbieders en door berichtensystemen gebruikte identificatiecodes.⁶⁰ Als deze informatie niet met technische middelen kan worden achterhaald, dient de CASP die informatie rechtstreeks van de initiator of begunstigde te verkrijgen.⁶¹ De CASP dient deze beoordeling te verrichten voordat de overdracht plaatsvindt.

Bij een overdracht van cryptoactiva naar of vanuit een zelfgehost adres, dient de CASP van de initiator of de CASP van de begunstigde de in artikel 14, eerste en tweede lid, TFR bedoelde informatie te verzamelen en te bewaren. De CASP dient er tevens voor te zorgen dat elke overdracht van cryptoactiva individueel kan worden geïdentificeerd.⁶² Dit geldt ook voor overdrachten van €1.000 of minder.

3.4.3. Overdracht van meer dan €1.000

In het geval van een overdracht ten bedrage van meer dan €1.000 naar of vanuit een zelfgehost adres, geldt er een aanvullende verplichting ter verificatie of het zelfgehoste adres eigendom is van of onder zeggenschap staat van de initiator, respectievelijk de begunstigde. De CASP van de initiator of de CASP van de begunstigde

⁵⁹ In overeenstemming met richtsnoer 87 van de Reisregelrichtsnoeren. Hierbij dient de CASP ten minste één van de risicobeperkende maatregelen als bedoeld in artikel 19bis, eerste lid, van Richtlijn (EU) 2015/849 toe te passen op een manier die in verhouding staat tot de vastgestelde risico's.

⁶⁰ Richtsnoer 77 e.v. van de Reisregelrichtsnoeren.

⁶¹ Richtsnoer 78 van de Reisregelrichtsnoeren.

⁶² Artikel 14, vijfde lid, TFR en artikel 16, tweede lid, TFR.

dienen passende maatregelen te nemen om dit te beoordelen.⁶³ De passende maatregelen moeten in het beleid en de procedures van de CASP worden vastgelegd. Onderdeel van het beleid en de procedures moet ook zijn de opsporing van overmakingen die met elkaar in verband lijken te staan en daarmee de drempel van meer dan €1.000 halen.⁶⁴

De verificatie door de CASP bij overdrachten van meer dan €1.000 dient plaats te vinden door toepassing van ten minste één van de volgende verificatiemethoden:⁶⁵

- a) Verificatie zonder menselijke tussenkomst;⁶⁶
- b) Verificatie met menselijke tussenkomst;⁶⁷
- c) Overmaking van een vooraf door de CASP bepaald bedrag van en naar het zelfgehoste adres op de rekening van de CASP;
- d) Een verzoek aan de cliënt om een specifiek bericht in de rekening- en portemonneesoftware digitaal te ondertekenen met de sleutel die overeenkomt met dat adres;
- e) Andere geschikte technische middelen, zolang deze een betrouwbare en beveiligde beoordeling mogelijk maken en de CASP met volle overtuiging weet wiens eigendom het adres is of onder wiens zeggenschap het staat.

Zoals hiervoor uiteengezet, dient de CASP in haar beleid vast te leggen van welke verificatiemethode zij gebruik maakt indien één verificatiemethode niet afdoende is. Wanneer de CASP heeft vastgesteld dat een zelfgehost adres eigendom is van of gecontroleerd wordt door haar cliënt, dient de CASP dit te documenteren en hoeft zij de bovenstaande maatregelen mogelijk niet opnieuw toe te passen op volgende transacties van of naar hetzelfde adres ('*whitelisting*').⁶⁸

3.4.4. Overdracht van en naar derden

Indien wordt vastgesteld dat een zelfgehost adres eigendom is van of onder zeggenschap staat van een derde persoon in plaats van de cliënt van de CASP, bestaat er een verhoogd risico op witwassen of het financieren van terrorisme. In dergelijke gevallen dient de CASP ter verificatie aanvullende maatregelen te treffen.⁶⁹ Ook dient de CASP in dat geval te beoordelen of de betrokkenheid van deze derde persoon aanleiding geeft tot aanvullende witwas- of terrorismefinanciering risico's. Indien dit het geval is, treft zij aanvullende (cliëntonderzoek)maatregelen om de risico's op witwassen en terrorismefinanciering te beperken en effectief te beheersen en om (indien hiertoe aanleiding is) ongebruikelijke transacties te melden bij de FIU-Nederland.

3.5. Herhaaldelijk nalatige CASPs en meldplicht

In voorgaande paragrafen is beschreven dat CASPs onderling gehouden zijn informatie te delen in de gevallen verplicht gesteld door de TFR. Indien informatie door de ene CASP bij de andere CASP wordt opgevraagd en de CASP is herhaaldelijk nalatig deze informatie te verstrekken, geldt hiertoe een meldplicht. Van de CASP wordt

⁶³ Artikel 14, vijfde lid, jo. artikel 16, tweede lid, TFR. Om te bepalen of de waarde 1 000 EUR of meer bedraagt, dient de CASP de wisselkoers van het over te dragen cryptoactief te gebruiken om de waarde ervan in euro's op het tijdstip van de overdracht te berekenen, eventuele transactiekosten buiten beschouwing gelaten.

⁶⁴ Richtsnoer 17 e.v. van de Reisregelrichtsnoeren.

⁶⁵ Richtsnoer 83 van de Reisregelrichtsnoeren.

⁶⁶ Zoals gespecificeerd in de richtsnoeren voor het gebruik van oplossingen voor de acceptatie van cliënten op afstand overeenkomstig artikel 13, eerste lid, van Richtlijn (EU) 2015/849, waarbij het adres wordt weergegeven.

⁶⁷ Idem.

⁶⁸ Richtsnoer 86 van de Reisregelrichtsnoeren. Een CASP die gebruikmaakt van whitelisting moet controles hebben om veranderingen in het ML/TF-risico van het zelf gehoste adres en het eigendom of de zeggenschap ervan te identificeren. Als de CASP vaststelt dat het ML/TF-risico van het zelfgehoste adres is veranderd of dat er aanwijzingen zijn dat haar klant niet langer eigenaar is van of zeggenschap heeft over het zelfgehoste adres, dient zij dit adres van haar witte lijst te verwijderen.

⁶⁹ Richtsnoer 89 van de Reisregelrichtsnoeren.

verwacht dat zij in beleid en procedures vastlegt hoe zij invulling geeft aan de meldplicht in het geval van ontbrekende, vereiste informatie.

Zo dient de CASP in de eerste plaats te beschikken over doeltreffende, op haar risicobeoordeling gebaseerde procedures om te beslissen wat de vereiste vervolgactie is die zij moet verbinden bij het ontbreken van de vereiste volledige informatie.⁷⁰ Indien een CASP herhaaldelijk in verzuim is om vereiste informatie te verstrekken⁷¹, kan een (intermediaire) CASP alle (toekomstige) overdrachten of zakelijke betrekkingen met die CASP weigeren, beperken of beëindigen.⁷² Dit kan zij direct doen of eerst waarschuwen. Het definiëren van herhaaldelijk verzuim en hoe hierop te handelen, moet zijn opgenomen in het beleid en de procedures van de (intermediaire) CASP.⁷³

Het herhaaldelijk verzuim om vereiste informatie te verstrekken moet onverwijld⁷⁴ aan de AFM worden gemeld. Onverwijld houdt in uiterlijk drie maanden nadat het herhaaldelijk verzuim door de (intermediaire) CASP is vastgesteld.⁷⁵ De melding moet plaatsvinden ongeacht de redenen om de schending te rechtvaardigen, en ongeacht of de in verzuim zijnde (intermediaire) CASP in de Unie dan wel daarbuiten gevestigd is.⁷⁶

Meldingen worden ingediend door een e-mail te sturen aan crypto@afm.nl onder vermelding van Melding verzuim TFR.⁷⁷ De AFM verzoekt deze e-mail toe te sturen met gebruik van Cryptshare.⁷⁸ Bij deze melding voegt de CASP het ingevulde (intermediaire) CASP-meldformulier toe, dat te vinden is op [Meldingsplichten voor CASPs](#).

3.5.1. Inhoud van de melding

De melding dient de volgende gegevens te bevatten⁷⁹:

- a) de naam van de (intermediaire) CASP waarvan is vastgesteld dat die herhaaldelijk heeft nagelaten vereiste informatie te verstrekken;
- b) het land waar de (intermediaire) CASP een vergunning heeft;
- c) de aard van de schending, waaronder:
 - i. de frequentie van overmakingen/overdrachten met ontbrekende informatie,
 - ii. de periode waarin de schendingen zijn vastgesteld, en
 - iii. eventuele redenen die de (intermediaire) CASP heeft gegeven ter rechtvaardiging van het herhaaldelijke verzuim om de vereiste informatie te verstrekken;
- d) details over de maatregelen die de meldende (intermediaire) CASP heeft ondernomen.

3.5.2. Onverwijld melden van een ongebruikelijke transactie bij FIU-Nederland

Het ontbreken van informatie van de initiator of de begunstigde bij overdrachten van cryptoactiva kan ook reden zijn tot het doen van een melding van een ongebruikelijke transactie bij de FIU-Nederland. De (intermediaire) CASP beoordeelt zelf of sprake is van een ongebruikelijke transactie, rekening houdend met de criteria die zijn vastgelegd in Europees recht, nationale wetgeving en in hun eigen interne beleid en

⁷⁰ Artikel 17, eerste lid TFR en artikel 21, eerste lid, TFR.

⁷¹ De Reisregelrichtsnoeren geven nadere invulling aan de deadlines bij het verzoek om informatie aan de CASP die in verzuim is. Zie Richtsnoer 56.

⁷² Artikel 17, tweede lid, TFR jo. artikel 21, tweede lid, TFR.

⁷³ Richtsnoeren 67 t/m 69 van de Reisregelrichtsnoeren.

⁷⁴ Richtsnoeren 74 en 75 van de Reisregelrichtsnoeren geven nadere invulling aan de meldverplichting, zie ook het vervolg van deze paragraaf.

⁷⁵ Richtsnoer 74 van de Reisregelrichtsnoeren.

⁷⁶ Richtsnoer 74 van de Reisregelrichtsnoeren.

⁷⁷ De verplichting voor het doen van de melding staat in artikel 17, tweede lid, TFR en in artikel 21, tweede lid, TFR.

⁷⁸ [Veilig bestanden uitwisselen \(Cryptshare\)](#)

⁷⁹ Richtsnoer 75 van de Reisregelrichtsnoeren.

procedures. Net als andere Wwft-instellingen dient een CASP een ongebruikelijke transactie onverwijld te melden bij FIU-Nederland. In paragraaf 6.2 van Leidraad wordt hier nader op ingegaan.

3.6. Aandachtspunten AVG

De AVG⁸⁰ is van toepassing voor de verwerking van persoonsgegevens bij overdrachten van cryptoactiva.⁸¹ De bestrijding van witwassen en terrorismefinanciering wordt erkend als een zwaarwegend algemeen belang. CASPs moeten ervoor zorgen dat de overdracht van persoonsgegevens van de betrokken partijen bij een overdracht van cryptoactiva altijd in overeenstemming is met de AVG.

CASPs opereren vaak in meerdere rechtsgebieden, ook buiten de Unie. Echter dient de CASP te allen tijde te voldoen aan haar verplichtingen in het kader van AML/CFT. Daarom is het met name van belang voor CASPs die in meerdere rechtsgebieden actief zijn, zich ervan te verzekeren dat zij niet worden belet in het doorgeven van informatie omtrent ongebruikelijke transacties binnen dezelfde organisatie. Verwacht wordt dat CASPs maatregelen treffen om dit te waarborgen. Zij moeten daarnaast beschikken over passende technische en organisatorische maatregelen voor de bescherming van persoonsgegevens tegen incidenteel verlies, wijziging, ongeoorloofde verspreiding of toegang.

⁸⁰ Verordening (EU) 2016/679.

⁸¹ Zie onder meer 14, vierde lid, TFR.

Bijlage – overzicht relevante wetgeving

Verordening (EU) 2023/1113 van het Europese Parlement en de Raad van 31 mei 2023 betreffende bij geldovermakingen en overdrachten van bepaalde cryptoactiva te voegen informatie en tot wijziging van Richtlijn (EU) 2015/849: [Regulation - 2023/1113 - EN - EUR-Lex](#)

EBA-richtsnoeren betreffende informatievereisten met betrekking tot geldovermakingen en bepaalde overdrachten van cryptoactiva uit hoofde van Verordening (EU) 2023/1113 (“reisregelrichtsnoeren”): [Travel Rule Guidelines.pdf](#)

EBA-richtsnoeren die richtsnoeren *EBA/2021/02 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions* (‘The ML/TF Risk Factors Guidelines’) under Articles 17 and 18(4) of Directive (EU) 2015/849 aanpassen: [Final Amending Guidelines on MLTF Risk Factors.pdf](#)

EBA-richtsnoeren “Guidelines on Internal Policies, procedures and controls to ensure the implementation of Union and national restrictive measures: addressed to financial institutions (EBA/GL/2024/14)”: [Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures | European Banking Authority](#).

Wwft: [wetten.nl - Regeling - Wet ter voorkoming van witwassen en financieren van terrorisme - BWBR0024282](#)

Uitvoeringsbesluit Wwft: [wetten.nl - Regeling - Uitvoeringsbesluit Wwft 2018 - BWBR0041193](#)

Uitvoeringsregeling Wwft: [wetten.nl - Regeling - Uitvoeringsregeling Wet ter voorkoming van witwassen en financieren van terrorisme - BWBR0024275](#)

Sanctiewet 1977: [wetten.nl - Regeling - Sanctiewet 1977 - BWBR0003296](#)

Regeling toezicht Sanctiewet 1977: [wetten.nl - Regeling - Regeling toezicht Sanctiewet 1977 - BWBR0018806](#)

**Autoriteit Financiële markten**

Postbus 11723 | 1001 GS Amsterdam

Telefoon

020 797 2000

www.afm.nl

Dataclassificatie

AFM-Publiek

Volg ons: →



De AFM maakt zich sterk voor eerlijke en transparante financiële markten.

Als onafhankelijke gedragstoezichthouder dragen wij bij aan duurzaam financieel welzijn in Nederland.

De tekst van deze publicatie is met zorg samengesteld en is informatief van aard. U kunt er geen rechten aan ontleen. Door veranderende wet- en regelgeving op nationaal en internationaal niveau is het mogelijk dat de tekst niet actueel is op het moment dat u deze leest. De Autoriteit Financiële Markten (AFM) is niet aansprakelijk voor de eventuele gevolgen – bijvoorbeeld geleden verlies of gederfde winst – ontstaan door of in verband met acties ondernomen naar aanleiding van deze tekst.

© Copyright AFM 2025