

De AFM heeft vandaag een [bijlage](#) op haar Leidraad Wwft en Sanctiewet gepubliceerd met aandachtspunten voor crypto-activadienstverleners (CASPs). Deze bijlage bestaat uit aandachtspunten voor CASPs ten opzichte van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft), de Sanctiewet 1977 (Sanctiewet), de Transfer of Funds Regulation (TFR) en de Algemene Verordening Gegevensbescherming. De Leidraad zelf blijft uiteraard onverkort gelden, maar de specifieke aandachtspunten voor CASPs bieden een nuttig overzicht van het toepasselijke juridisch kader. Hieronder bespreken wij drie key take-aways.

Key take-away 1: risicobeoordeling

De AFM geeft aan dat zij verwacht van een CASP dat de meest recente [nationale risicobeoordeling \(NRA\)](#) wordt betrokken in de risicobeoordeling. Uit de NRA blijkt dat witwassen via CASPs één van de achttien grootste witwasdreigingen in Nederland is, waardoor de AFM veel verwacht van de risicobeoordeling van CASPs en de risico-beheersende maatregelen. De risicobeoordeling mag volgens de AFM niet beperkt worden tot abstracte en algemeen geformuleerde risico's, maar moet juist zo concreet mogelijk. Het moet dus worden toegespitst op onder meer de specifieke diensten en cliënten van de CASP, verrijkt met data ter ondersteuning van de risico's.

Key take-away 2: self-hosted adressen

De AFM schenkt ook bijzondere aandacht aan diensten waarbij self-hosted adressen betrokken zijn, zowel in het kader van de Wwft, de Sanctiewet, als onder TFR. Deze diensten gaan namelijk gepaard met potentieel hoge integriteitsrisico's, waardoor risicobeperkende maatregelen moeten worden getroffen. Van CASP wordt daarom verwacht dat zij:

- een risicobeoordeling uitvoeren om te bepalen wanneer er een meer dan minimaal risico bestaat dat financiële middelen ter beschikking worden gesteld aan personen of entiteiten die op een sanctielijst staan.
- beleid implementeren omtrent de verificatie van de identiteit van personen met eigendom/zeggenschap over self-hosted adressen, inclusief het moment waarop verificatie wordt uitgevoerd en de gebruikte verificatiemethoden.
- extra alertheid tonen wanneer het adres onder zeggenschap van een derde staat in plaats van de cliënt.

Key take-away 3: TFR beleid

Aan de TFR wordt in de bijlage bijzondere aandacht besteedt. Dat is ook niet gek, nu de TFR voor CASPs een grotere rol speelt dan voor PSPs, waarvoor deze vereisten al langere tijd gelden. Dit komt omdat de traceerbaarheid bij crypto-activa minder vanzelfsprekend is dan bij het overmaken van geldmiddelen.

Uiteraard verwacht de AFM dat CASPs de TFR in hun beleid en procedures opnemen. Daarin moet onder meer worden vastgelegd welke transacties binnen het TFR-toepassingsbereik vallen, inclusief wanneer de CASP optreedt als initiator of begunstigde. Dit beleid moet ook de gevolgen van onvolledige informatie bij een overdracht beschrijven, waaronder in welke gevallen een overdracht wordt uitgevoerd, geweigerd, teruggezonden of opgeschort.

Daarnaast moeten CASPs voor verzending en ontvangst van cryptoactiva infrastructuur en diensten gebruiken die technisch in staat zijn om informatie volledig en foutloos over te dragen.

Meer weten over het implementeren van de Leidraad en bijlage in CASP beleid? Neem contact op met ons crypto-team voor praktische ondersteuning.



Tim de Wit
Partner
tim.de.wit@finnius.com
M: +31 (0)6 110 045 26



Maurice van Oosten
Senior Associate
maurice.van.oosten@finnius.com
M: +31 (0)6 508 484 85



Daniëlle van de Vijver
Senior Associate
danielle.van.de.vijver@finnius.com
M: +31 (0)6 214 804 53



Marise Kok
Associate
marise.kok@finnius.com
M: +31 (0)6 252 982 99