Know Your Customer

KYC voor vermogensbeheerders



Inhoud

Identificatie en Verificatie voor Vermogensbeheerders: Een Cruciaal Proces 3
- Wie is de klant? 3
- Persoonsgegevens ontvangen 3
- Is de persoon in bezit van een geldig paspoort? 3
- Persoonsgegevens verifiëren aan de hand van paspoort 4

Groepsstructuur en UBO's vaststellen bij vermogensbeheerders 5

KYC voor Vermogensbeheerders: PEP, Sanctie en Adverse Media Screening 7

Risico-analyse volgens de WWFT 9

KYC bij Vermogensbeheerders: Ondertekening van de Overeenkomst 11

Periodieke Review en Monitoring in KYC voor Vermogensbeheerders 13

Identificatie en Verificatie voor Vermogensbeheerders: Een Cruciaal Proces

Binnen de financiële sector speelt het kennen van je klant (Know Your Customer, ofwel KYC) een vitale rol, vooral voor vermogensbeheerders die te maken hebben met hoge kapitalen en strikte regelgevingen. Dit proces begint met het identificeren van de klant.

Wie is de klant

De eerste stap in het KYC-proces is het vaststellen van de identiteit van de klant. Dit is niet enkel een kwestie van weten hoe de klant heet, maar ook van het begrijpen van de achtergrond, activiteiten en financiële geschiedenis van die klant. Het opbouwen van een volledig klantprofiel helpt vermogensbeheerders bij het evalueren van de risico's en het waarborgen van compliance met relevante wetten en regelgeving.

Persoonsgegevens ontvangen

Zodra er interactie is met een potentiële klant, is het verzamelen van hun persoonsgegevens een standaardprocedure. Deze gegevens kunnen bestaan uit naam, geboortedatum, adres, nationaliteit en andere relevante informatie. Deze gegevens zijn essentieel voor het opbouwen van een basisklantprofiel en het uitvoeren van verdere verificatieprocessen.

Is de persoon in bezit van een geldig paspoort?

De authenticiteit van de verstrekte gegevens wordt vaak geverifieerd aan de hand van officiële identificatiedocumenten. Een geldig paspoort is een van de meest geaccepteerde en betrouwbare vormen van identificatie wereldwijd. Het is de verantwoordelijkheid van de vermogensbeheerder om te bevestigen dat de klant in het bezit is van een geldig paspoort en dat dit document niet is verlopen of anderszins ongeldig is verklaard.

Persoonsgegevens verifiëren aan de hand van paspoort

De verstrekte persoonsgegevens moeten nauwkeurig worden vergeleken met de gegevens in het paspoort. Discrepanties, hoe klein ook, moeten worden opgehelderd. Dit kan betekenen dat aanvullende documentatie of verklaringen van de klant nodig zijn. De consistentie tussen de verstrekte informatie en het paspoort waarborgt niet alleen de authenticiteit van de klant, maar beschermt ook vermogensbeheerders tegen mogelijke fraude of witwasactiviteiten.

In conclusie, voor vermogensbeheerders is een grondige identificatie en verificatie van hun klanten van het grootste belang. Dit waarborgt niet alleen compliance en risicobeheer, maar beschermt ook het imago en de integriteit van hun bedrijf in een steeds complexer wordende financiële wereld.

Groepsstructuur en UBO’s vaststellen bij vermogensbeheerders

Voor vermogensbeheerders die zakelijke klanten bedienen, is het essentieel de groepsstructuur en de uiteindelijke begunstigde (UBO: Ultimate Beneficial Owner) van een onderneming te identificeren. Dit proces is een kritiek onderdeel van Know Your Customer (KYC) maatregelen, die gericht zijn op het voorkomen van witwassen en terrorismefinanciering.

Het inzichtelijk maken van de groepsstructuur is niet alleen van belang om te weten wie de daadwerkelijke beslissers zijn binnen de organisatie, maar ook om de verwevenheid van verschillende entiteiten en de daaruit voortvloeiende risico's te begrijpen. In sommige gevallen kan een groepsstructuur buitengewoon complex zijn, met meerdere lagen van dochterondernemingen, joint ventures en gelieerde entiteiten. Een bijzonder complexe groepsstructuur kan een indicator zijn van een hoger risico, vooral als de structuur is ontworpen om de ware eigendom of controle te verbergen.

De UBO is de natuurlijke persoon of personen die uiteindelijk eigenaar zijn van of zeggenschap hebben over een klant van de vermogensbeheerder, wanneer deze klant een rechtspersoon is. De definitie van een UBO kan variëren afhankelijk van de lokale wetgeving, maar over het algemeen gaat het om individuen die direct of indirect meer dan 25% van de eigendom of stemrechten van een entiteit bezitten, of die de entiteit controleren via andere middelen.

In situaties waar de UBO ook een directe klant van de vermogensbeheerder is, is het cruciaal om de belangen en verbindingen tussen de zakelijke en individuele relaties volledig te begrijpen. Hierbij gaat het niet alleen om de financiële belangen, maar ook om de invloed die de UBO kan uitoefenen op het beheer en de strategie van het vermogen.

Tot slot verdienen UBO’s met een internationale achtergrond extra aandacht. Er kunnen bijkomende uitdagingen zijn bij het verkrijgen van verifieerbare documentatie voor buitenlandse UBO’s, en er kunnen extra risico’s zijn geassocieerd met jurisdicties die minder strikte regelgevende en transparantienormen hanteren. Daarom is het voor vermogensbeheerders essentieel om robuuste procedures en controles te hebben bij het vaststellen van groepsstructuren en UBO’s, vooral in een internationale context.

KYC voor Vermogensbeheerders: PEP, Sanctie en Adverse Media Screening

Het kennen van je klant (KYC) is in de financiële wereld niet alleen essentieel voor het opbouwen van vertrouwen en het waarborgen van de integriteit van het financiële systeem, maar het is ook een juridische verplichting die voortvloeit uit de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) en andere internationale regelgevingen. Een van de kernaspecten van de KYC-procedures voor vermogensbeheerders is het screenen van klanten op basis van drie specifieke criteria: PEP-status, sancties en adverse media.

Screening op PEP status: Politiek prominente personen (PEP's) zijn individuen die een belangrijke openbare functie bekleden, of hebben bekleed, en hun directe familieleden en naaste geassocieerden. Door hun positie kunnen PEP's potentieel risico lopen om betrokken te raken bij corruptie. De PEP-screening zorgt ervoor dat vermogensbeheerders de bron van de activa van een PEP begrijpen en monitoren om te waarborgen dat ze geen gelden beheren die zijn verkregen uit illegale of corrupte bronnen. Dit helpt niet alleen bij het vermijden van reputatierisico's maar ook bij het voldoen aan wettelijke verplichtingen.

Screening op Sancties: Sancties zijn beperkingen die door landen of internationale organisaties worden opgelegd aan individuen, organisaties of landen om bepaalde gedragingen te ontmoedigen, zoals het schenden van mensenrechten, het financieren van terrorisme of het uitvoeren van massavernietigingswapens. Vermogensbeheerders zijn wettelijk verplicht om te verzekeren dat zij geen zakelijke relaties onderhouden of transacties uitvoeren met entiteiten of personen die op sanctielijsten staan. Sanctiescreening helpt vermogensbeheerders deze lijsten systematisch te controleren om te waarborgen dat zij volledig voldoen aan deze beperkingen.

Screening op adverse media: Media kunnen een rijke bron van informatie zijn over potentiële risico's verbonden aan een klant. Adverse media screening, of negatieve nieuws screening, verwijst naar het proces van het controleren van nieuwsbronnen en artikelen om te zien of een potentiële of bestaande klant in verband wordt gebracht met criminele activiteiten, corruptie, fraude of andere risicovolle zaken. Het identificeren van dergelijke risico's via media-inhoud stelt vermogensbeheerders in staat om geïnformeerde beslissingen te nemen over het al dan niet aangaan of voortzetten van een zakelijke relatie.

Samenvattend, in de context van KYC voor vermogensbeheerders, is het van cruciaal belang om deze drie screeningsmethoden toe te passen. Ze bieden een holistisch overzicht van potentiële risico's en stellen professionals in staat om passende maatregelen te nemen om de integriteit van hun operaties en het financiële systeem als geheel te waarborgen.

Risico-analyse volgens de WWFT

Binnen de financiële sector is het waarborgen van integriteit essentieel. De Wet ter voorkoming van witwassen en financieren van terrorisme (WWFT) beoogt een proactieve aanpak ter preventie van ongewenste financiële activiteiten. Een van de kritische stappen in deze aanpak is risico-analyse. Hieronder worden drie cruciale facetten van deze analyse onderzocht.

Persoonsgebonden risico's: Deze verwijzen naar de risico's die verbonden zijn aan de identiteit en de achtergrond van een cliënt. Vermogensbeheerders moeten cliënten grondig screenen om potentiële rode vlaggen te identificeren. Dit kan zijn een politiek prominente functie (PEP), ongebruikelijke bedrijfsactiviteiten, vage of indirecte antwoorden tijdens het KYC-proces of eerdere betrokkenheid bij financiële delicten. Grondige persoonsgebonden due diligence kan vermogensbeheerders helpen potentiële risico's in een vroeg stadium te identificeren en daardoor ongewenste associaties en activiteiten voorkomen.

Product- of transactiegebonden risico's: Niet alle financiële producten en transacties dragen hetzelfde risico. Complexere producten met een gebrek aan transparantie of transacties die specifiek zijn opgezet om de ware aard of herkomst van geld te verhullen, kunnen hogere risico's met zich meebrengen. Bijvoorbeeld, producten met een hoge mate van privacy of waarde die snel over de grenzen kan worden verplaatst, zoals bepaalde soorten derivaten of digitale valuta, kunnen meer risico met zich meebrengen. Vermogensbeheerders moeten hun productaanbod continu evalueren en cliënten monitoren om ervoor te zorgen dat zij geen producten gebruiken op een manier die ongebruikelijk of verdacht is.

Geografische risico's: Deze hebben betrekking op de landen en regio's waarin de cliënt actief is of waaruit zijn vermogen afkomstig is. Sommige landen hebben een hoger risico op witwassen of financiering van terrorisme vanwege zwakkere regelgeving, corruptie, of een geschiedenis van financiële onregelmatigheden. Landen op de 'zwarte lijst' of 'grijze lijst' van internationale financiële waakhonden, zoals de Financial Action Task Force (FATF), moeten met bijzondere voorzichtigheid worden benaderd. Vermogensbeheerders moeten zorgvuldig de geografische verbindingen van hun cliënten evalueren en overwegen of de risico's passend en beheersbaar zijn binnen hun risicotolerantie.

In conclusie vereist de WWFT dat vermogensbeheerders een gedetailleerde, gelaagde en holistische risicoanalyse uitvoeren. Door de bovengenoemde risico's zorgvuldig in overweging te nemen, kunnen zij niet alleen voldoen aan wettelijke vereisten, maar ook hun eigen reputatie en die van hun cliënten beschermen.

KYC bij Vermogensbeheerders: Ondertekening van de Overeenkomst

Het Know Your Customer (KYC) proces is een integraal onderdeel van de moderne financiële dienstverlening, vooral bij vermogensbeheerders. Dit proces waarborgt dat instellingen een grondig inzicht hebben in hun klanten, hun financiële activiteiten en, vooral, hun risicoprofiel. De ondertekening van de overeenkomst is een kritiek moment in dit proces en vereist nauwgezette aandacht om zowel wettelijke als operationele redenen.

Bij het **vastleggen van de overeenkomst** is het van cruciaal belang dat alle details nauwkeurig zijn vastgelegd. Dit omvat niet alleen de financiële modaliteiten zoals beheersvergoedingen, investeringsparameters en andere financiële voorwaarden, maar ook de persoonlijke details van de cliënt. Dit omvat niet alleen basisidentificatie zoals naam en adres, maar ook andere relevante details die specifiek zijn voor het KYC-proces, zoals bronnen van rijkdom, zakelijke belangen, enz. Deze details stellen vermogensbeheerders in staat om een accuraat risicoprofiel van de klant te vormen en zich aan te passen aan de regelgevende vereisten.

Een even kritieke vraag is echter of de **juiste persoon het document ondertekent**. Dit is niet alleen relevant vanuit een wettelijk perspectief, waar het essentieel is om ervoor te zorgen dat de ondertekenaar de wettelijke bevoegdheid heeft om namens de entiteit of het individu te handelen, maar ook vanuit een risicoperspectief. Foute identificaties of frauduleuze pogingen kunnen leiden tot significante operationele en juridische risico's voor de vermogensbeheerder. Daarom moeten vermogensbeheerders strenge identificatie- en verificatieprocedures implementeren, inclusief, maar niet beperkt tot, het controleren van identificatiedocumenten, het verifiëren van handtekeningen en, waar mogelijk, persoonlijke ontmoetingen.

In een wereld waar digitale interacties de norm worden, zijn ook digitale handtekeningtechnologieën en geavanceerde identificatie- en verificatietechnieken steeds relevanter geworden. Het combineren van deze technologieën met traditionele KYC-methoden kan vermogensbeheerders helpen bij het waarborgen van de integriteit van hun overeenkomsten en het minimaliseren van risico's.

Het KYC-proces is een continu en evoluerend landschap, vooral met de constant veranderende regelgevingsnormen en technologische vooruitgang. Als zodanig moeten vermogensbeheerders ervoor zorgen dat hun procedures en protocollen altijd up-to-date zijn, vooral tijdens kritieke interactiemomenten zoals de ondertekening van overeenkomsten.

Periodieke Review en Monitoring in KYC voor Vermogensbeheerders

Eén van de essentiële aspecten van het Know Your Customer (KYC) proces voor vermogensbeheerders is de periodieke review en monitoring van klantprofielen. Deze herbeoordeling verzekert de consistentie en de relevantie van de klantgegevens en speelt een cruciale rol bij het waarborgen van een effectief anti-witwasbeleid (AWB).

Afhankelijk van het risiconiveau geassocieerd met elke klant, is het van vitaal belang om op vastgestelde intervallen een risico-onderzoek uit te voeren. Klanten met een hoger risicoprofiel, bijvoorbeeld vanwege hun geografische locatie, de aard van hun activiteiten, of het type van hun transacties, vereisen wellicht frequentere en diepgaandere evaluaties. Een periodieke herziening stelt vermogensbeheerders in staat om veranderende omstandigheden of activiteiten te identificeren die mogelijk een verschuiving in het risiconiveau van de klant aangeven.

Een ander essentieel facet van deze periodieke controle is het monitoren van de herkomst van de geldstromen. Dit zorgt ervoor dat vermogensbeheerders verdachte transacties of ongebruikelijke patronen kunnen identificeren die in strijd zijn met de oorspronkelijk verstrekte klantinformatie, of die wijzen op mogelijk misbruik of financiële criminaliteit.

De hoogte van vermogens is ook een significant aandachtspunt. Plotselinge en substantiële toenames in het vermogen van een klant, zonder een duidelijke en legitieme verklaring, kunnen rode vlaggen zijn voor onregelmatigheden of ongeoorloofde activiteiten. Hetzelfde geldt voor onverklaarbare schommelingen in vermogen, wat kan duiden op frequente grote stortingen en opnames, wat vaak wordt geassocieerd met witwaspraktijken.

In conclusie, het is voor vermogensbeheerders van essentieel belang om een robuuste en dynamische KYC-procedure te hebben. Periodieke review en monitoring, afgestemd op het risiconiveau van elke klant, zijn onmisbare tools om financiële integriteit en compliance te waarborgen in een steeds veranderende financiële wereld.