

NALEVINGSRICHTLIJNEN TEGEN HET WITWASSEN VAN GELD EN DE FINANCIERING VAN TERRORISME

INLEIDING	2
DEFINITIES.....	3
PRINCIPES VOOR STRUCTUUR EN BESTUUR VAN HET BEDRIJF	6
DE RAAD VAN BESTUUR.....	6
DE EERSTE VERDEDIGINGSLINIE - DE WERKNEMERS	6
DE TWEEDE VERDEDIGINGSLINIE - RISICOBEBEER EN NALEVING, MLRO	7
DE DERDE VERDEDIGINGSLINIE - INTERNE AUDIT	8
BEGINSELEN VAN DE IMPLEMENTATIE VAN KLANTENONDERZOEKSMATREGELEN.....	9
BELANGRIJKSTE PRINCIPES.....	9
DE GELEVERDE DIENSTEN.....	10
DE VERIFICATIE VAN INFORMATIE DIE WORDT GEBRUIKT VOOR DE IDENTIFICATIE VAN DE KLANT	10
TOEPASSING VAN VEREENVOUDIGDE DUE DILIGENCE-MATREGELEN(NIVEAU 1).....	11
TOEPASSING VAN STANDAARDONDERZOEKSMATREGELEN (NIVEAU 2).....	12
TOEPASSING VAN VERSCHERPTE DUE DILIGENCE-MATREGELEN (NIVEAU 3)	12
KLANTENONDERZOEKSMATREGELEN	15
IDENTIFICATIE VAN DE KLANT - NATUURLIJKE PERSOON.....	16
IDENTIFICATIE VAN DE KLANT - JURIDISCHE ENTITEIT.....	16
DE IDENTIFICATIE VAN DE VERTEGENWOORDIGER VAN DE KLANT EN ZIJN RECHT VAN VERTEGENWOORDIGING	17
DE IDENTIFICATIE VAN DE WETTELIJK EIGENAAR VAN DE KLANT	17
POLITIEKE ONTMASKERINGPERSOONSIDENTIFICATIE	19
IDENTIFICATIE VAN HET DOEL EN DE AARD VAN DE ZAKELIJKE RELATIE OF TRANSACTIE	21
CONTROLE VAN DE ZAKENRELATIE.....	22
UITVOERING VAN SANCTIES.....	24
PROCEDURE VOOR HET IDENTIFICEREN VAN HET VOORWERP VAN SANCTIES EN EEN TRANSACTIE DIE SANCTIES SCHENDT	24
ACTIES BIJ HET IDENTIFICEREN VAN HET SANCTIEONDERWERP OF EEN TRANSACTIE DIE SANCTIES SCHENDT	25
WEIGERING VAN DE TRANSACTIE OF ZAKELIJKE RELATIE EN DE BEËINDIGING ERVAN	26
MELDINGSPLICHT	26
MELDINGSPLICHT VOOR SPECIFIEKE SOORTEN TRANSACTIES.....	27
TRAININGSVERPLICHTING	28
VERZAMELEN EN OPSLAAN VAN GEGEVENS, LOGBOEKEN	29
REGISTRATIE LOGBOEKEN BIJHOUDEN.....	30
PROCEDURE VOOR HET BIJHOUDEN EN BEHEREN VAN REGISTRATIELOGBOEKEN	32
INTERNE CONTROLE OP DE UITVOERING VAN DE RICHTLIJNEN.....	33
RISICOBEOORDELING EN RISICOBEREIDHEID	35
IMPLEMENTATIE VAN KLANTENONDERZOEKSMATREGELEN	35
UITVOERING VAN SANCTIES	36
VERPLICHTING TOT WEIGERING VAN TRANSACTIE OF ZAKELIJKE RELATIE EN DE BEËINDIGING ERVAN	36
RAPPORTAGEVERPLICHTING.....	36
TRAININGSVERPLICHTING.....	36
VERPLICHTING TOT HET VERZAMELEN EN BEWAREN VAN GEGEVENS.....	36
BIJLAGEN	38
VERSIEBEHEER TABEL	39

INLEIDING

Het doel van deze richtlijnen voor antiwitwasmaatregelen (AML), maatregelen ter bestrijding van terrorismefinanciering (CFT) en sancties is om ervoor te zorgen dat **UAB Criptomys** (Onderneming) interne richtlijnen heeft om het gebruik van haar bedrijf voor het witwassen van geld en terrorismefinanciering te voorkomen en interne richtlijnen voor de implementatie van internationale sancties.

Deze Richtlijnen zijn aangenomen om ervoor te zorgen dat het Bedrijf de regels en voorschriften naleeft die zijn vastgelegd in de Wet ter voorkoming van het witwassen van geld en de financiering van terrorisme (Wet) van de Republiek Litouwen en andere toepasselijke wetgeving, waaronder de volgende:

- Technische vereisten voor het proces van klantenidentificatie voor authenticatie op afstand via elektronische apparaten voor directe videotransmissie, goedgekeurd door de directeur van de Dienst voor onderzoek naar financiële criminaliteit van het ministerie van Binnenlandse Zaken van de Republiek Litouwen op 30 november 2016 bij Resolutie nr. V-314 "Voor de technische vereisten voor het proces van klantenidentificatie voor authenticatie op afstand via elektronische apparaten voor directe videotransmissie" (hierna - Technische vereisten).¹
- Resolutie nr. V-240 van 5 december 2014 van de directeur van de onderzoeksdienst financiële criminaliteit van het ministerie van Binnenlandse Zaken van de Republiek Litouwen "inzake de goedkeuring van de lijst met criteria voor het witwassen van geld en de identificatie van verdachte of ongebruikelijke monetaire verrichtingen of transacties".²
- Resolutie nr. V-5 van 10 januari 2020 van de Directeur van de Dienst Onderzoek naar Financiële Criminaliteit van het Ministerie van Binnenlandse Zaken van de Republiek Litouwen "Over de goedkeuring van richtlijnen voor de beheerders van portemonnees van virtuele valuta en beheerders van wisselkantoren van virtuele valuta om het witwassen van geld en/of de financiering van terrorisme te voorkomen".³
- Resolutie nr. V-273 van 20 oktober 2016 van de directeur van de onderzoeksdienst financiële criminaliteit van het ministerie van Binnenlandse Zaken van de Republiek Litouwen "inzake de goedkeuring van richtsnoeren voor het toezicht op financiële misdrijven voor de tenuitvoerlegging van internationale financiële sancties op het gebied van verordeningen van het ministerie van Binnenlandse Zaken van de Republiek Litouwen".⁴
- De minister van Binnenlandse Zaken van de Republiek Litouwen 2017 16 oktober bij Besluit nr. 1V- 701 "inzake opschorting van verdachte monetaire transacties of transacties en indiening van informatie over verdachte monetaire transacties of transacties bij de dienst onderzoek financiële criminaliteit volgens de procedurebeschrijving van het ministerie van Binnenlandse Zaken van de Republiek Litouwen en informatie over contante transacties of transacties van 15.000 euro of meer of indiening van het overeenkomstige bedrag in buitenlandse valuta".

¹ <https://www.e-tar.lt/portal/lt/legalAct/e45f4270b70011e6aae49c0b9525cbbb/asr>

² <https://www.e-tar.lt/portal/lt/legalAct/a664b2107ecd11e4bc68a1493830b8b9>

³ <https://www.e-tar.lt/portal/lt/legalAct/570a231035e011ea829bc2bea81c1194>

⁴ <https://www.e-tar.lt/portal/lt/legalAct/01d5d4e0974411e69ad4c8713b612d0f>

Munteenheid aan de Dienst Onderzoek Financiële Criminaliteit onder goedkeuring van de beschrijving van de procedure van het Ministerie van Binnenlandse Zaken van de Republiek Litouwen "⁵

- Directeur van de Dienst Onderzoek Financiële Criminaliteit 2015 21 mei bij beschikking nr. V-129 "betreffende de goedkeuring van informatieformulieren, indieningsschema's en aanbevelingen voor het invullen van informatie die wordt verstrekt in overeenstemming met de vereisten van de wet ter voorkoming van het witwassen van geld en de financiering van terrorisme van de Republiek Litouwen".⁶

Deze Richtlijnen worden ten minste jaarlijks herzien door de Directie. Voorstellen voor een herziening en de herziening van deze richtlijnen kunnen vaker worden gepland bij besluit van de Money Laundering Reporting Officer (MLRO) of de Internal Control Officer van het bedrijf.

Deze Richtlijnen worden aanvaard en goedgekeurd bij besluit van de Raad van Bestuur van het Bedrijf.

DEFINITIES

Beneficial Owner betekent een natuurlijke persoon die, profiterend van zijn invloed, een transactie, handeling, actie of stap uitvoert of op een andere manier controle uitoefent over een transactie, handeling, actie of stap of over een andere persoon en in wiens belang of ten gunste of voor wiens rekening een transactie of handeling, actie of stap wordt uitgevoerd. In het geval van een rechtspersoon is de Begunstigde Eigenaar een natuurlijke persoon wiens directe of indirecte deelneming, of de som van alle directe en indirecte deelnemingen in de rechtspersoon, meer dan 25 procent bedraagt, inclusief deelnemingen in de vorm van aandelen of andere vormen van aan toonder.

Zakelijke relatie betekent een relatie die tot stand komt na het sluiten van een langetermijncontract door het Bedrijf in economische of professionele activiteiten met als doel het leveren van een dienst of de distributie ervan op een andere manier of die niet gebaseerd is op een langetermijncontract, maar waarbij een bepaalde duur redelijkerwijs verwacht kon worden op het moment van het tot stand brengen van het contact en gedurende welke het Bedrijf herhaaldelijk afzonderlijke transacties uitvoert in het kader van economische of professionele activiteiten tijdens het leveren van een dienst.

Bedrijf betekent rechtspersoon met de volgende gegevens:

- bedrijfsnaam: UAB CRYPTOMY;
- Land van registratie: Litouwen;
- registratienummer: 306127858;
- adres: Vilnius, Eišiškių Sodų 18-oji g. 11;
- e-mail: info@criptomy.exchange, contact@criptomy.exchange

Bewaarder Virtual Currency Wallet betekent Virtual Currency Adres(sen) gegenereerd met de publieke sleutel⁷ voor het opslaan en beheren van Virtual Currencies die aan het Bedrijf zijn toevertrouwd, maar hun eigendom blijven.

⁵ <https://e-tar.lt/portal/lt/legalAct/143ad320b24011e7afdadc0e4460de4>

⁶ <https://www.e-tar.lt/portal/lt/legalAct/e1f42fa0006d11e588da8908dfa91cac>

Bewaarder Virtual Currency Wallet betekent Virtual Currency Adres(sen) gegenereerd met de publieke sleutel⁷ voor het opslaan en beheren van Virtual Currencies die aan het Bedrijf zijn toevertrouwd, maar hun eigendom blijven.

Klant betekent een natuurlijke persoon of een rechtspersoon die een Zakelijke Relatie met het Bedrijf heeft.

Werknemer betekent de werknemer van het Bedrijf en elke andere persoon die betrokken is bij de toepassing van deze Richtlijnen in het Bedrijf.

Richtlijnen - dit document inclusief alle bijlagen zoals hierboven vermeld. De richtlijnen omvatten onder andere de interne controleprocedure van het bedrijf met betrekking tot de richtlijnen en het risicobeoordelingsbeleid van het bedrijf met betrekking tot de risicogebaseerde aanpak voor ML/TF-risico's.

Raad van Bestuur betekent de raad van bestuur van het Bedrijf. Als het bedrijf geen raad van bestuur heeft, wordt de manager van het bedrijf beschouwd als lid van de raad van bestuur en is hij of zij verantwoordelijk voor de taken van de raad van bestuur in het kader van de richtlijnen.

MLRO betekent Money Laundering Reporting Officer, die bij het bedrijf is aangesteld als een persoon die verantwoordelijk is voor het ontvangen van interne meldingen en het maken van rapporten aan de Financial Crime Investigation Service (FCIS) en andere taken zoals hierboven beschreven.

Monetaire Operatie betekent elke betaling, overdracht of ontvangst van geld.

Het witwassen van geld (Money Laundering, ML) is het verbergen van de herkomst van illegaal geld door het in het legale economische systeem te brengen en door transacties die legitiem lijken. Er zijn drie erkende stadia in het witwasproces:

- plaatsing, waarbij de opbrengsten van misdrijven in het financiële systeem worden geplaatst;
- layering, waarbij de opbrengsten van misdrijven in een andere vorm worden omgezet en complexe lagen van financiële transacties worden gecreëerd om het controlespoor en de bron en het eigendom van de fondsen te verhullen;
- integratie, waarbij de witgewassen opbrengsten terug in de economie worden gestopt om de perceptie van legitimiteit te creëren.

Incidentele Transactie betekent de transactie die door het Bedrijf wordt uitgevoerd in het kader van economische of professionele activiteiten met als doel het leveren van een dienst of de verkoop van goederen of de distributie daarvan op een andere manier aan de Klant buiten de loop van een vastgestelde Zakelijke Relatie.

PEP betekent een natuurlijke persoon die prominente publieke functies uitoefent of heeft uitgeoefend en ten aanzien van wie er gerelateerde risico's blijven bestaan.

Sancties zijn een essentieel instrument van het buitenlands beleid ter ondersteuning van het behoud of herstel van vrede, internationale veiligheid, democratie en de rechtsstaat, in navolging van de mensenrechten.

⁷ **Publieke sleutel** betekent een code van letters, cijfers en/of symbolen die is ontworpen om de klant te identificeren en het adres van de virtuele valuta van de klant te genereren.

Rechten en het internationaal recht of het bereiken van andere doelstellingen van het Handvest van de Verenigde Naties of het gemeenschappelijk buitenlands en veiligheidsbeleid van de Europese Unie. Sancties omvatten:

- internationale Sancties tegen een staat, grondgebied, territoriale eenheid, regime, organisatie, vereniging, groep of persoon uit hoofde van een resolutie van de Veiligheidsraad van de Verenigde Naties, een besluit van de Raad van de Europese Unie of enige andere wetgeving die verplichtingen oplegt aan Litouwen;
- Sancties van de regering van de Republiek Litouwen die een instrument van buitenlands beleid zijn en die naast de in de vorige zin genoemde doelstellingen kunnen worden opgelegd om de veiligheid of de belangen van Litouwen te beschermen.

Internationale sancties kunnen de binnenkomst van een subject van een internationale sanctie in de staat verbieden, internationale handel en internationale transacties beperken, en andere verboden of verplichtingen opleggen.

Het voorwerp van sancties is elke natuurlijke of rechtspersoon, entiteit of lichaam, aangewezen in de rechtshandeling die sancties oplegt of implementeert, waarop de sancties van toepassing zijn.

Financiering van terrorisme (Terrorist Financing, TF): het financieren en ondersteunen van een terroristische daad en het plegen van deze daad, evenals het financieren en ondersteunen van reizen ten behoeve van terrorisme in de zin van de toepasselijke wetgeving.

Derde land betekent een staat die geen lid is van de Europese Economische Ruimte (EER).

Virtuele valuta: een waarde die wordt vertegenwoordigd in digitale vorm, die digitaal overdraagbaar, houdbaar of verhandelbaar is en die natuurlijke personen of rechtspersonen aanvaarden als betaalinstrument, maar die niet het wettig betaalmiddel is van een land of geldmiddelen in de zin van artikel 4, punt 25, van Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad betreffende betalingsdiensten in de interne markt, tot wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening (EU) nr. 1093/2010, en tot intrekking van Richtlijn 2007/64/EG (PB L 337 van 23. 12. 2015, blz. 35-127) of een betalingstransactie in de zin van artikel 3, onder k) en l), van dezelfde richtlijn.12.2015, blz. 35-127) of een betalingstransactie in de zin van artikel 3, onder k) en l), van dezelfde richtlijn.

Virtuele Valuta Adres: adres/rekening gegenereerd uit letters, cijfers en/of symbolen in de blockchain, waarmee de blockchain de Virtuele Valuta toewijst aan de eigenaar of ontvanger.

PRINCIPES VOOR STRUCTUUR EN MANAGEMENT VAN HET BEDRIJF

De organisatiestructuur van het bedrijf moet overeenkomen met haar omvang en de aard, reikwijdte en complexiteit van haar activiteiten en geleverde diensten, inclusief de risicobereidheid en gerelateerde risico's, en moet gestructureerd zijn volgens het principe **van drie verdedigingslijnes**. De organisatiestructuur van het bedrijf moet overeenkomen met het volledige inzicht in potentiële risico's en het beheer ervan. De rapportage- en ondergeschiktheidsketens van het Bedrijf moeten zodanig zijn dat alle Medewerkers hun plaats in de organisatiestructuur kennen en hun taken kennen.

De raad van bestuur

De raad van bestuur is de drager van de cultuur van naleving van de vereisten voor de preventie van het witwassen van geld en de financiering van terrorisme, en garandeert dat de leden van de raad van bestuur en de werknemers van het bedrijf werken in een omgeving waarin zij volledig op de hoogte zijn van de vereisten voor de preventie van het witwassen van geld en de financiering van terrorisme en de verplichtingen die aan deze vereisten verbonden zijn, en waarin in gepaste mate rekening wordt gehouden met de relevante risico-overwegingen in de besluitvormingsprocessen van het bedrijf.

De leden van de raad van bestuur dragen de eindverantwoordelijkheid voor de maatregelen die worden genomen om het gebruik van de diensten van het bedrijf voor het witwassen van geld of de financiering van terrorisme te voorkomen. Zij houden toezicht en zijn verantwoordelijk voor:

- vaststellen en onderhouden van AML⁸ processen, procedures, risico- en controleprocessen;
- het aannemen van deze Richtlijnen en andere interne richtlijnen en instructies;
- het bepalen van de richtlijnen van het bedrijf voor AML-maatregelen;
- het benoemen van een MLRO en ervoor te zorgen dat de MLRO over de bevoegdheden, middelen en deskundigheid beschikt die nodig zijn om hun opdracht uit te voeren;
- het toewijzen van voldoende middelen om de effectieve implementatie van de Richtlijnen en andere gerelateerde documenten te waarborgen en de organisatie in stand te houden;
- ervoor zorgen dat alle relevante medewerkers de jaarlijkse AML-training voltooien.

De eerste verdedigingslinie - de werknemers

De eerste verdedigingslinie heeft de functie van het toepassen van de zorgvuldigheidseisen bij het aangaan van een Zakelijke Relatie en het toepassen van zorgvuldigheidseisen tijdens de Zakelijke Relatie. De eerste verdedigingslinie bestaat uit de structurele eenheden en Werknemers van het Bedrijf aan wier activiteiten risico's verbonden zijn en die deze risico's, hun specifieke kenmerken en reikwijdte moeten identificeren en beoordelen en die deze risico's beheren door middel van hun gewone activiteiten, voornamelijk door due diligence maatregelen toe te passen. De risico's die voortvloeien uit de activiteiten van en dienstverlening door het Bedrijf behoren tot de eerste verdedigingslinie. Zij zijn de beheerders (eigenaren) van deze risico's en zijn er verantwoordelijk voor.

⁸ Ter vereenvoudiging van deze Richtlijnen wordt onder "AML" ook het voorkomen van terrorismefinanciering en het implementeren van sancties verstaan.

De Werknemers van het Bedrijf moeten handelen met de vooruitziendheid en competentie die van hen verwacht wordt en volgens de vereisten die gesteld zijn voor hun posities, uitgaande van de belangen en doelen van het Bedrijf, en ervoor zorgen dat het financiële systeem en de economische ruimte van het land niet gebruikt worden voor het witwassen van geld en de financiering van terrorisme. Het bedrijf neemt maatregelen om de geschiktheid van de werknemers te beoordelen voordat zij aan de slag gaan met de relevante training.

Om bovengenoemde redenen zijn de Werknemers verplicht om:

- alle vereisten naleven die in de Richtlijnen en andere gerelateerde documenten staan;
- de vereiste klantinformatie verzamelen in overeenstemming met hun functie en verantwoordelijkheden;
- informatie, situaties, activiteiten, transacties of pogingen tot transacties melden die ongebruikelijk zijn voor elk type dienst of klantrelatie, ongeacht het bedrag, ongeacht of de transactie onverwijld werd voltooid of niet;
- Klanten niet informeren of anderszins op de hoogte stellen als de Klant of andere Klanten het onderwerp zijn of kunnen zijn van een rapport of als er een rapport is of kan worden ingediend;
- de juiste AML-training voltooien die vereist is voor de functie van de werknemer.

De tweede verdedigingslinie - Risicobeheer en naleving, MLRO

De tweede verdedigingslinie bestaat uit de risicomanagement- en compliancefuncties. Deze functies kunnen ook door dezelfde persoon of structurele eenheid worden uitgevoerd, afhankelijk van de grootte van het bedrijf en de aard, reikwijdte en mate van complexiteit van hun activiteiten en verleende diensten, inclusief de risicobereidheid en risico's die voortvloeien uit activiteiten van het bedrijf.

Het doel van de **compliancefunctie** is om te garanderen dat het Bedrijf de geldende wetgeving, richtlijnen en andere documenten naleeft en om het mogelijke effect van wijzigingen in de wettelijke of regelgevende omgeving op de activiteiten van het Bedrijf en op het compliancekader te beoordelen. De taak van compliance is om de eerste verdedigingslinie als de eigenaren van risico's te helpen bij het bepalen van de plaatsen waar risico's zich manifesteren (bijv. analyse van verdachte en ongebruikelijke transacties, waarvoor compliance-medewerkers de vereiste professionele vaardigheden, persoonlijke kwaliteiten, enz. hebben) en om de eerste verdedigingslinie te helpen deze risico's efficiënt te beheren. De tweede verdedigingslinie neemt geen risico's.

Het risicobeleid wordt uitgevoerd en het kader voor risicobeheer wordt gecontroleerd door de **risicobeheerfunctie**. De uitvoerder van de risicobeheerfunctie zorgt ervoor dat alle risico's worden geïdentificeerd, beoordeeld, gemeten, bewaakt en beheerd, en informeert de betreffende eenheden van het bedrijf hierover. De uitvoerder van de risicobeheerfunctie voor AML houdt voornamelijk toezicht op de naleving van de risicobereidheid, toezicht op de risicotolerantie, toezicht op de identificatie van wijzigingen in risico's, houdt een overzicht van de bijbehorende risico's en voert andere taken uit die verband houden met risicobeheer.

De Raad van Bestuur heeft een **MLRO** aangesteld voor het uitvoeren van de tweedelijns verdedigingsfuncties. Deze persoon is niet operationeel betrokken bij de gebieden die de MLRO zal controleren en verifiëren en is dus onafhankelijk met betrekking tot deze gebieden.

Binnen het huidige AML-kader van het bedrijf is het de MLRO die de belangrijkste beslissingen neemt over individuele AML-kwesties, zoals het goedkeuren van PEP's, het accepteren of weigeren van gebruikers met een hoog risico. enz. De aangewezen AML-functionaris van het bedrijf is de senior functionaris van het bedrijf en een persoon die over alle noodzakelijke kennis en werkachtergrond beschikt.

De MLRO is verantwoordelijk voor de volgende activiteiten:

- de Richtlijnen van het Bedrijf opstellen en, indien nodig, bijwerken;
- doorlopend controleren en verifiëren of het Bedrijf voldoet aan de vereisten die worden voorgeschreven door deze Richtlijnen en verwante documenten en volgens externe wet- en regelgeving;
- het personeel van het bedrijf en de leden van de Raad van Bestuur advies en ondersteuning bieden met betrekking tot de regels inzake het witwassen van geld en terrorismefinanciering;
- de leden van de raad van bestuur en relevante personen informeren en opleiden over de regels met betrekking tot het witwassen van geld en terrorismefinanciering;
- voldoende gegevens over ontvangen interne meldingen onderzoeken en registreren en beslissen of de activiteit gerechtvaardigd of verdacht is;
- de relevante rapporten in te dienen bij de betreffende regelgevende instanties in overeenstemming met de toepasselijke wetgeving;
- controleren en regelmatig beoordelen of de procedures en richtlijnen van het bedrijf ter voorkoming van het gebruik van het bedrijf voor het witwassen van geld of de financiering van terrorisme geschikt en effectief zijn.

De MLRO rapporteert elk kwartaal aan de raad van bestuur. Dit rapport moet schriftelijk zijn en ten minste de volgende punten bevatten:

- aantal Klanten in alle risicoklassen
- aantal treffers voor personen in verband met de sanctielijsten en toegepaste maatregelen;
- aantal Klanten of vertegenwoordigers van Klanten die geïdentificeerd zijn als PEP's of personen met een connectie met een PEP;
- aantal interne meldingen over verdachte activiteiten of transacties;
- aantal van de relevante meldingen aan de Financial Crime Investigation Service (FCIS);
- aantal en inhoud van een verzoek om informatie van het FCIS in het kader van een onderzoek;
- bevestiging dat de risicobeoordeling van het bedrijf voor het witwassen van geld en de financiering van terrorisme up-to-date is;
- bevestiging dat deze Richtlijnen en andere gerelateerde documenten up-to-date zijn;
- bevestiging dat er voldoende personeel is voor AML-maatregelen;
- alle (eventuele) tekortkomingen die door de controlefunctie zijn geïdentificeerd, zijn aangepakt;
- lijst van verplichte trainingen die zijn gehouden voor het personeel met betrekking tot AML-maatregelen

De derde verdedigingslinie - Interne controle

De derde verdedigingslinie wordt gevormd door de onafhankelijke en effectieve interne auditfunctie. De interne auditfunctie kan worden uitgevoerd door een interne controlefunctionaris. Dit kan een of meerdere werknemers zijn, de structurele eenheid van het Bedrijf met de relevante functies of een derde partij die de relevante dienst aan het Bedrijf levert. Het is de interne controleur niet toegestaan om de functie van MLRO en/of lid van de raad van bestuur van het bedrijf te bekleden of enige andere functie die het opstellen en/of redigeren van de interne regels en richtlijnen van het bedrijf met betrekking tot het witwassen van geld en de financiering van terrorisme omvat.

De werknemers, de structurele eenheid van het Bedrijf of een derde partij die de interne auditfunctie uitvoert, moeten beschikken over de vereiste competentie, hulpmiddelen en toegang tot de relevante informatie in alle structurele eenheden van het Bedrijf. De interne auditmethoden moeten in overeenstemming zijn met de grootte van het Bedrijf, de aard, reikwijdte en mate van complexiteit van de activiteiten en verleende diensten, inclusief de risicobereidheid en risico's die voortvloeien uit activiteiten van het Bedrijf.

Het besluit om een interne audit uit te voeren wordt genomen door de raad van bestuur. De Raad van Bestuur moet minstens één keer per jaar beoordelen of een interne audit nodig is.

PRINCIPES VOOR DE IMPLEMENTATIE VAN KLANTENONDERZOEKSMATREGELEN

Customer due diligence (CDD)-maatregelen zijn vereist voor het verifiëren van de identiteit van een nieuwe of bestaande klant als een goed uitgevoerde risicogebaseerde doorlopende controle van de zakelijke relatie met de klant. De CDD-maatregelen bestaan uit 3 niveaus, waaronder vereenvoudigde en verscherpte due diligence-maatregelen, zoals hieronder gespecificeerd.

Belangrijkste principes

De CDD-maatregelen worden in de volgende gevallen genomen en uitgevoerd voor zover dat nodig is gezien het risicoprofiel van de Klant en andere omstandigheden:

- bij het aangaan van de Zakelijke Relatie en tijdens de voortdurende controle van de Zakelijke Relatie;
- bij het uitvoeren of bemiddelen van Occasionele Transactie(s) buiten de Zakelijke Relatie, waarbij de waarde van de transactie(s) 700 euro of meer bedraagt (of een gelijk bedrag in andere activa) binnen 24 uur;
- bij het uitvoeren of bemiddelen van Occasionele Transactie(s) buiten de Zakelijke Relatie, waarbij de waarde van de transactie(s) binnen een maand 10.000 euro of meer bedraagt (of een gelijk bedrag in andere activa);
- na verificatie van informatie die is verzameld tijdens de toepassing van due diligence-maatregelen of in geval van twijfel over de toereikendheid of waarachtigheid van de eerder verzamelde documenten of gegevens tijdens het bijwerken van de relevante gegevens;
- op verdenking van het witwassen van geld of de financiering van terrorisme, ongeacht eventuele afwijkingen, uitzonderingen of beperkingen die in deze richtlijnen en de toepasselijke wetgeving zijn vastgelegd.

Het Bedrijf brengt de Zakelijke Relatie niet tot stand en onderhoudt deze niet en voert de transactie niet uit als:

- is het Bedrijf niet in staat om de vereiste CDD-maatregelen te nemen en uit te voeren;
- het Bedrijf vermoedens heeft dat de diensten of transactie van het Bedrijf zullen worden gebruikt voor het witwassen van geld of de financiering van terrorisme;
- het risiconiveau van de Klant of van de transactie niet in overeenstemming is met de risicobereidheid van het Bedrijf.

In het geval van het ontvangen van informatie in vreemde talen in het kader van CDD-implementatie, kan het bedrijf verzoeken om vertaling van de documenten in een andere taal die geschikt is voor het bedrijf. Het gebruik van vertalingen moet worden vermeden in situaties waarin de originele documenten zijn opgesteld in een taal die geschikt is voor het bedrijf.

Het bereiken van CDD is een proces dat begint met de implementatie van CDD-maatregelen. Als dat proces is voltooid, krijgt de Klant een gedocumenteerd individueel risiconiveau toegewezen dat de basis vormt voor vervolgmaatregelen, en dat indien nodig wordt opgevolgd en bijgewerkt.

Het bedrijf heeft CDD-maatregelen adequaat toegepast als het bedrijf de innerlijke overtuiging heeft dat het heeft voldaan aan de verplichting om due diligence-maatregelen toe te passen. Het principe van redelijkheid wordt in acht genomen bij de overweging van innerlijke overtuiging. Dit betekent dat het Bedrijf, bij de toepassing van CDD-maatregelen, de kennis, het begrip en de bevestiging moet hebben dat ze voldoende informatie hebben verzameld over de Klant, de activiteiten van de Klant, het doel van de Zakelijke Relatie en van de transacties die worden uitgevoerd in het kader van de Zakelijke Relatie, de herkomst van de fondsen, etc., zodat ze de Klant en de (zakelijke) activiteiten van de Klant begrijpen, daarbij rekening houdend met het risiconiveau van de Klant, het risico dat verbonden is aan de Zakelijke Relatie en de aard van deze relatie. Een dergelijk niveau van bevestiging moet het mogelijk maken om ingewikkelde, waardevolle en ongebruikelijke transacties en transactiepatronen te identificeren die geen redelijk of voor de hand liggend economisch of legitiem doel hebben of die niet kenmerkend zijn voor de specifieke kenmerken van de zakelijke relatie in kwestie.

Het bedrijf moet CDD niet alleen toepassen op natuurlijke personen, maar ook op rechtspersonen. Alle tegenpartijen en partners van het bedrijf worden handmatig gecontroleerd door de MLRO Officer met behulp van betrouwbare en onafhankelijke bronnen.

De geleverde diensten

De belangrijkste economische activiteit van het Bedrijf zijn de Virtuele Valutadiensten. Daarom biedt het Bedrijf haar Klanten de volgende transactietypen aan:

- het aanbieden van Virtual Currency exchange operator service, waarmee de Klant Virtual Currency kan inwisselen, kopen en verkopen.

Het Bedrijf zal de bovengenoemde diensten alleen verlenen in het kader van een bestaande Zakelijke Relatie.

De verificatie van informatie die wordt gebruikt voor de identificatie van de Klant

Verificatie van de informatie voor de identificatie van de Klant betekent dat gegevens uit een betrouwbare en onafhankelijke bron worden gebruikt om te bevestigen dat de gegevens waarheidsgetrouw en correct zijn, waarbij indien nodig ook wordt bevestigd dat de gegevens die rechtstreeks betrekking hebben op de Klant waarheidsgetrouw en correct zijn. Dit betekent onder andere dat het doel van de informatieverificatie is om er zeker van te zijn dat de Klant,

- die afkomstig is van twee verschillende bronnen;
- die is uitgegeven door (identiteitsdocumenten) of ontvangen van een derde partij of een plaats die geen belang heeft bij of banden onderhoudt met de Klant of het Bedrijf, d.w.z. die neutraal is (bijv. informatie verkregen van internet is niet dergelijke informatie, aangezien deze vaak afkomstig is van de Klant zelf of de betrouwbaarheid en onafhankelijkheid ervan niet kan worden gecontroleerd);
- waarvan de betrouwbaarheid en onafhankelijkheid zonder objectieve hindernissen kan worden vastgesteld en waarvan de betrouwbaarheid en onafhankelijkheid ook begrijpelijk zijn voor een derde partij die niet betrokken is bij de Zakelijke relatie; en
- de gegevens die erin zijn opgenomen of via welke zijn verkregen, actueel en relevant zijn en het Bedrijf hierover zekerheid kan verkrijgen (en zekerheid kan in bepaalde gevallen ook verkregen worden op basis van de twee voorgaande clausules).

Toepassing van vereenvoudigde due diligence-maatregelen (niveau 1)

Vereenvoudigde due diligence (SDD)-maatregelen worden toegepast als het risicoprofiel van de klant wijst op een laag risiconiveau van ML/TF.

Bij het toepassen van SDD-maatregelen mag het Bedrijf alleen de volgende gegevens van de Klant, die een natuurlijke persoon is, verkrijgen⁹ :

- naam/namen en achternaam/namen;
- persoonlijk nummer;¹⁰ of

in het geval van de Klant, die een rechtspersoon is, de volgende gegevens:

- bedrijfsnaam of naam;
- rechtsvorm;
- registratienummer, indien een dergelijk nummer is uitgegeven;
- hoofdkantoor (adres) en adres van de feitelijke activiteit;
- de representatieve naam/namen, achternaam/namen en het persoonsnummer of de geboortedatum van de Klant; en

ervoor zorgen dat de eerste betaling wordt uitgevoerd via een rekening bij een kredietinstelling, waarbij de kredietinstelling geregistreerd is in de EER of in een derde land dat eisen stelt die gelijkwaardig zijn aan de eisen die in de relevante wetgeving zijn vastgelegd en dat door bevoegde autoriteiten toezicht wordt gehouden op de naleving van deze eisen.

SDD-maatregelen mogen alleen worden uitgevoerd als de voortdurende controle van de Zakelijke Relatie van de Klant wordt uitgevoerd in overeenstemming met de Richtlijnen en er een mogelijkheid is om verdachte Geldtransacties en transacties te identificeren.

SDD-maatregelen mogen niet worden uitgevoerd in de omstandigheden waarin verscherpte due diligence-maatregelen (zoals hieronder beschreven) moeten worden uitgevoerd.

⁹ Wanneer de klant een staats- of gemeentelijke instelling of agentschap of de Bank van Litouwen is, kan het Bedrijf tijdens het toepassen van SDD-maatregelen alleen persoonlijke nummers van dergelijke entiteiten en hun vertegenwoordiger verzamelen.

¹⁰ in het geval van een buitenlander - geboortedatum (indien beschikbaar - persoonlijk nummer of een andere unieke reeks symbolen die aan die persoon is toegekend, bedoeld voor persoonlijke identificatie).

Wanneer tijdens het uitvoeren van voortdurende controle van de Zakelijke Relaties van de Klant wordt vastgesteld dat het risico op ML en/of TF niet langer laag is, moet het Bedrijf het relevante niveau van CDD-maatregelen toepassen.

Toepassing van standaard due diligence-maatregelen (niveau 2)

Standaard due diligence-maatregelen worden toegepast op alle Klanten waarbij CDD-maatregelen moeten worden toegepast in overeenstemming met de Richtlijnen. De volgende standaard due diligence maatregelen moeten worden toegepast:

- identificatie van de Klant en verificatie van de ingediende informatie op basis van informatie verkregen van een betrouwbare en onafhankelijke bron;
- identificatie en verificatie van een vertegenwoordiger van de Klant en zijn recht op vertegenwoordiging;
- identificatie van de Begunstigde Eigenaar en, met het oog op het verifiëren van hun identiteit, het nemen van maatregelen in die mate dat het Bedrijf er zeker van kan zijn dat het weet wie de Begunstigde Eigenaar is, en de eigendoms- en controlestructuur van de Klant begrijpt;
- inzicht in de Zakelijke relatie, transactie of operatie en, indien relevant, het verzamelen van informatie daarover;
- informatie verzamelen over de vraag of de Klant een PEP is, een familielid of een persoon die bekend staat als een naaste medewerker;
- controle van de zakenrelatie.

De hierboven gespecificeerde CDD-maatregelen moeten worden toegepast voordat de zakelijke relatie wordt aangegaan of de transactie wordt uitgevoerd. De exacte instructies voor de toepassing van standaard due diligence maatregelen staan in de Richtlijnen.

Toepassing van verscherpte due diligence-maatregelen (niveau 3)

Naast de standaard due diligence-maatregelen past het bedrijf verscherpte due diligence-maatregelen (EDD) toe om een vastgesteld risico op het witwassen van geld en de financiering van terrorisme te beheren en te beperken in het geval het risico hoger is dan normaal.

Het bedrijf past altijd EDD-maatregelen toe wanneer:

- het risicoprofiel van de Klant wijst op een hoog risiconiveau van ML / TF;
- na identificatie van de Klant of verificatie van ingediende informatie, er twijfel bestaat over de waarheidsgetrouwheid van de ingediende gegevens, de authenticiteit van de documenten of de identificatie van de Beneficial Owner;
- wanneer grensoverschrijdende correspondentrelaties worden aangegaan met de Klant, die een financiële instelling van een Derde Land is;
- in het geval van het uitvoeren van een transactie of zakelijke relatie met de PEP, het familielid van de PEP of een persoon waarvan bekend is dat hij een nauwe relatie heeft met de PEP;
- wanneer transacties of Zakelijke Relaties worden uitgevoerd met natuurlijke personen die woonachtig zijn of rechtspersonen die gevestigd zijn in Derde Landen met een hoog risico zoals geïdentificeerd door de Europese Commissie;

- de Klant afkomstig is uit een dergelijk land of gebied of zijn woonplaats of zetel of de zetel van de betalingsdienstaanbieder van de begunstigde zich in een land of gebied bevindt dat, volgens geloofwaardige bronnen zoals wederzijdse evaluaties, rapporten of gepubliceerde opvolgingsrapporten, geen doeltreffende systemen ter bestrijding van witwassen en financiering van terrorisme heeft opgezet die in overeenstemming zijn met de aanbevelingen van de FATF.

Alvorens EDD-maatregelen toe te passen, zorgt de Medewerker van het Bedrijf ervoor dat de Zakelijke Relatie of transactie een hoog risico heeft en dat een hoog risicopercantage kan worden toegeschreven aan een dergelijke Zakelijke Relatie of transactie. Bovenal beoordeelt de Medewerker voorafgaand aan het toepassen van de EDD-maatregelen of de hierboven beschreven kenmerken aanwezig zijn en past deze als onafhankelijke gronden toe (dat wil zeggen dat elk van de geïdentificeerde factoren toepassing van EDD-maatregelen met betrekking tot de Klant mogelijk maakt).

Bij het toepassen van EDD-maatregelen wanneer een grensoverschrijdende correspondentrelatie wordt aangegaan met de Klant, die een financiële instelling uit een derde land is, moet het Bedrijf de volgende maatregelen toepassen:

- voldoende informatie over de Klant verzamelen om de aard van zijn activiteiten volledig te begrijpen en om op basis van openbaar beschikbare informatie de reputatie van de Klant en de kwaliteit van het toezicht vast te stellen;
- controlemechanismen voor AML van de Klant en de entiteit die fondsen ontvangt, beoordelen;
- goedkeuring verkrijgen van het bestuurslid voordat nieuwe correspondentrelaties worden aangegaan;
- de respectieve verantwoordelijkheden van de Klant documenteren;
- ervan overtuigd zijn dat de Klant de juiste "Customer due diligence" heeft uitgevoerd (met inbegrip van het verifiëren van de identiteit van de Klanten die directe toegang hebben tot de rekeningen van de Klant en het uitvoeren van andere "Customer due diligence" handelingen) en dat hij in staat is om de relevante Klantidentificatiegegevens op verzoek van het Bedrijf aan het Bedrijf te verstrekken.

Bij het toepassen van EDD-maatregelen, wanneer transacties of zakelijke relaties worden uitgevoerd met de PEP, het familielid van de PEP of een persoon waarvan bekend is dat hij een nauwe band heeft met de PEP, moet het bedrijf de volgende maatregelen toepassen:

- goedkeuring verkrijgen van het lid van de Raad van Bestuur alvorens een Zakelijke Relatie aan te gaan met een dergelijke Klant of de Zakelijke Relatie met de Klant voort te zetten wanneer hij of zij een PEP wordt;
- adequate maatregelen nemen om de bron van rijkdom en de bron van fondsen vast te stellen die betrokken zijn bij de Zakelijke relatie of transactie;
- de Bedrijfsrelatie met de Klant voortdurend controleren door het aantal en de timing van de toegepaste controles te verhogen, en transactiepatronen te selecteren die nader onderzocht moeten worden.

Bij het toepassen van EDD-maatregelen waarbij transacties of Zakelijke Relaties worden uitgevoerd met natuurlijke personen die woonachtig zijn of rechtspersonen die gevestigd zijn in Derde Landen met een hoog risico zoals geïdentificeerd door de Europese Commissie, moet het Bedrijf de volgende maatregelen toepassen:

- het verkrijgen van aanvullende informatie over de Klant en zijn Beneficial Owner;
- het verkrijgen van aanvullende informatie over de beoogde aard van de Zakelijke Relatie;
- het verkrijgen van informatie over de bron van fondsen en de bron van rijkdom van de Klant en hun Beneficial Owner;
- het verkrijgen van informatie over de redenen voor de voorgenomen of uitgevoerde transacties;
- het verkrijgen van goedkeuring van het lid van de Raad van Bestuur voor het aangaan van Zakelijke Relaties met de Klant of het voortzetten van Zakelijke Relaties met hen;
- de Bedrijfsrelatie met de Klant voortdurend controleren door het aantal en de timing van de toegepaste controles te verhogen, en transactiepatronen te selecteren die nader onderzocht moeten worden;
- ervoor zorgen dat de eerste betaling wordt uitgevoerd via een rekening op naam van de Klant bij een kredietinstelling, waarbij de kredietinstelling geregistreerd is in de EER of in een derde land dat eisen stelt die gelijkwaardig zijn aan de eisen die in de toepasselijke wetgeving zijn vastgelegd en dat door bevoegde autoriteiten toezicht wordt gehouden op de naleving van deze eisen.

Bij het toepassen van EDD-maatregelen waarbij de klant uit een dergelijk land of gebied komt of zijn woonplaats of zetel of de zetel van de betalingsdienstaanbieder van de begunstigde zich in een land of gebied bevindt dat, volgens geloofwaardige bronnen zoals wederzijdse evaluaties, rapporten of gepubliceerde follow-upverslagen, geen effectieve AML/CFT-systemen heeft opgezet die in overeenstemming zijn met de aanbevelingen van de FATF, moet de onderneming de volgende maatregelen toepassen:

- het verkrijgen van goedkeuring van het lid van de Raad van Bestuur voor het aangaan van Zakelijke Relaties met de Klant of het voortzetten van Zakelijke Relaties met hen;
- het verkrijgen van informatie over de bron van fondsen en de bron van rijkdom van de Klant en hun Beneficial Owner;
- de Bedrijfsrelatie met de Klant voortdurend controleren door het aantal en de timing van de toegepaste controles te verhogen, en transactiepatronen te selecteren die nader onderzocht moeten worden;

In alle andere gevallen waarin EDD-maatregelen moeten worden toegepast, wordt de omvang van de EDD-maatregelen en de reikwijdte bepaald door de Werknemer die dergelijke maatregelen toepast. De volgende aanvullende en relevante due diligence-maatregelen kunnen worden gevolgd:

- verificatie van aanvullend ingediende informatie na identificatie van de Klant op basis van aanvullende documenten, gegevens of informatie afkomstig van een geloofwaardige en onafhankelijke bron;
- aanvullende informatie verzamelen over het doel en de aard van de Zakelijke relatie of transactie en de ingediende informatie verifiëren op basis van aanvullende documenten, gegevens of informatie die afkomstig is van een betrouwbare en onafhankelijke bron;
- het verzamelen van aanvullende informatie en documenten om de bron en oorsprong van de fondsen die gebruikt zijn in een transactie in de Zakelijke Relatie te identificeren om de schijnbaarheid van de transacties uit te sluiten;
- het verrichten van de eerste betaling met betrekking tot een transactie via een rekening die geopend op naam van de Klant die deelneemt aan de transactie bij een kredietinstelling die geregistreerd is of haar zetel heeft in een overeenkomstsluitende staat van de Europese Economische Ruimte of in een land waar vereisten van kracht zijn die gelijk zijn aan die van Richtlijn (EU) 2015/849 van het Europees Parlement en de Raad;

- de toepassing van CDD-maatregelen met betrekking tot de Klant of zijn vertegenwoordiger, terwijl hij zich op dezelfde plaats bevindt als de Klant of zijn vertegenwoordiger;
- het verzamelen van aanvullende informatie over de Klant en zijn Beneficial Owner, inclusief de identificatie van alle eigenaren van de Klant, inclusief degenen wier aandelenbezit minder dan 25% is;
- informatie verzamelen over de herkomst van de fondsen en het vermogen van de Klant en zijn Beneficial Owner;
- het verbeteren van het toezicht op de Zakenrelatie door het aantal en de frequentie van de toegepaste controlemaatregelen te verhogen en door transactie-indicatoren of transactiepatronen te kiezen die extra gecontroleerd worden;
- het verkrijgen van goedkeuring van het lid van de Raad van Bestuur voor het uitvoeren van transacties of het aangaan van zakelijke relaties met nieuwe en bestaande Klanten;

Bij het uitvoeren van EDD is het Bedrijf in bepaalde gevallen verplicht om redelijke maatregelen te nemen om de bron van fondsen en de bron van rijkdom van de Klanten vast te stellen. De bron van de fondsen kan worden geverifieerd aan de hand van, *onder andere*:

- een jaarlijkse belastingaangifte;
- een origineel of gewaarmerkt afschrift van een recent loonstrookje;
- schriftelijke bevestiging van het jaarsalaris, ondertekend door een werkgever;
- een origineel of gewaarmerkt afschrift van het verkoopcontract van het onroerend goed en een origineel uittreksel van een financiële instelling waaruit de ontvangst blijkt van fondsen verkregen uit de verkoop van het onroerend goed, indien beschikbaar;
- een origineel of gewaarmerkt afschrift van een testament of een gelijkwaardig document waaruit de erfenis blijkt;
- een origineel of gewaarmerkt afschrift van een schenkingsovereenkomst (in een eenvoudige schriftelijke vorm, of gewaarmerkt door een notaris als de wet een notariële vorm van de overeenkomst vereist);
- een origineel of gewaarmerkt afschrift van een leningsovereenkomst (in een eenvoudige schriftelijke vorm, of gewaarmerkt door een notaris indien de wet een notariële overeenkomst vereist), en een uittreksel van een financiële instelling waaruit de ontvangst of verzending van fondsen in verband met de ontvangst van de lening of de terugbetaling van een verstrekte lening blijkt; of een promesse (in een eenvoudige schriftelijke vorm, of gewaarmerkt door een notaris indien de wet een notariële overeenkomst vereist);
- een zoekopdracht op internet in een bedrijfsregister om de verkoop van een bedrijf te bevestigen;
- origineel of een gewaarmerkt afschrift van de deposito-overeenkomst;
- kasboek of kasverrichtingenregister (voor rechtspersonen);
- overige informatie.

De werknemer stelt de MLRO binnen 2 werkdagen na het begin van de toepassing van de EDD-maatregelen op de hoogte van de toegepaste EDD-maatregelen door relevante kennisgeving te sturen.

Bij toepassing van EDD-maatregelen beoordeelt het Bedrijf het risicoprofiel van de Klant uiterlijk elke zes maanden opnieuw.

KLANTENONDERZOEKSMATREGELEN

Identificatie van de Klant - natuurlijke persoon

Het Bedrijf identificeert de Klant die een natuurlijke persoon is en, indien van toepassing, zijn vertegenwoordiger en bewaart de volgende gegevens over de Klant:

- naam/namen en achternaam/namen;
- persoonlijk nummer;¹¹
- burgerschap;¹²
- foto;
- handtekening.¹³

De volgende geldige identiteitsdocumenten die de hierboven vermelde gegevens bevatten, kunnen worden gebruikt als basis voor de identificatie van een natuurlijke persoon:

- een identiteitsbewijs van de Republiek Litouwen met uitzondering van een verblijfsvergunning van de Republiek Litouwen;
- een identiteitsbewijs van een buitenlandse staat;

De Klant, die een natuurlijk persoon is, kan geen gebruik maken van een vertegenwoordiger in het kader van de Zakelijke Relatie met het Bedrijf.

Identificatie van de Klant - rechtspersoon

Het Bedrijf identificeert de Klant die een rechtspersoon is en zijn vertegenwoordiger en bewaart de volgende gegevens over de Klant:

- bedrijfsnaam of naam;
- rechtsvorm;
- registratienummer, indien een dergelijk nummer is uitgegeven;

¹¹ in het geval van een buitenlander - geboortedatum (indien beschikbaar - persoonlijk nummer of een andere unieke reeks symbolen die aan die persoon is toegekend, bedoeld voor persoonlijke identificatie);

¹² wanneer een identiteitsdocument geen gegevens over het staatsburgerschap van de klant bevat, moeten financiële instellingen en andere verplichte entiteiten bij het identificeren van de klant die een natuurlijke persoon is in de fysieke aanwezigheid van de klant, de klant vragen om de gegevens over het staatsburgerschap te verstrekken.

¹³ behalve in de gevallen waarin het optioneel is in het identiteitsdocument;

- naam/namen en achterna(a)m(en), persoonlijk nummer (in het geval van een buitenlander - geboortedatum of indien beschikbaar - persoonlijk nummer of een andere unieke reeks symbolen toegekend aan

die persoon, bedoeld voor persoonlijke identificatie) en nationaliteit van de directeur(en) of lid (leden) van de Raad van Bestuur of lid (leden) van een ander gelijkwaardig orgaan, en hun bevoegdheden om de Klant te vertegenwoordigen;

- een registratie-uittreksel en de datum van afgifte;
- hoofdkantoor (adres) en adres van feitelijke activiteit
- Voor de identificatie van de Klant kunnen de volgende documenten worden gebruikt, die niet eerder dan zes maanden voor het gebruik ervan door een bevoegde autoriteit of instantie zijn afgegeven:
 - registerkaart van het desbetreffende register; of
 - inschrijvingsbewijs van het desbetreffende register; of
 - een document dat gelijkwaardig is met bovengenoemde documenten of relevante documenten van vestiging van de Klant.

Het Bedrijf controleert de juistheid van de hierboven vermelde gegevens van de Klant en gebruikt daarvoor informatie afkomstig van een geloofwaardige en onafhankelijke bron. Als het Bedrijf toegang heeft tot het relevante rechtspersonenregister, hoeft de Klant niet te worden verzocht om de bovengenoemde documenten in te dienen.

De identiteit van de rechtspersoon en het recht van vertegenwoordiging van de rechtspersoon kunnen worden geverifieerd aan de hand van een hierboven gespecificeerd document dat door een notaris is gewaarmerkt of gecertificeerd of officieel, of aan de hand van andere informatie afkomstig van een geloofwaardige en onafhankelijke bron, inclusief middelen voor elektronische identificatie en vertrouwensdiensten voor elektronische transacties, waarbij in een dergelijk geval ten minste twee verschillende bronnen voor de verificatie van gegevens worden gebruikt.

De identificatie van de vertegenwoordiger van de Klant en zijn recht op vertegenwoordiging

De vertegenwoordiger van de Klant wordt geïdentificeerd als de Klant, die een natuurlijke persoon is in overeenstemming met deze Richtlijnen. Het Bedrijf moet ook de aard en de reikwijdte van het vertegenwoordigingsrecht van de Klant vaststellen en verifiëren. De naam, datum van uitgifte en naam van de uitgevende instelling van het document dat als basis dient voor het recht van vertegenwoordiging moet worden vastgesteld en bewaard, behalve in het geval dat het recht van vertegenwoordiging werd geverifieerd aan de hand van informatie afkomstig uit het betreffende register.

Het Bedrijf moet zich houden aan de voorwaarden van het vertegenwoordigingsrecht dat is toegekend aan de vertegenwoordigers van de rechtspersoon en alleen diensten verlenen binnen de reikwijdte van het vertegenwoordigingsrecht.

De machtiging moet in overeenstemming zijn met de vereisten van het Litouwse Burgerlijk Wetboek. De in het buitenland afgegeven machtiging moet gelegaliseerd zijn of voorzien van een apostille. Indien het recht van vertegenwoordiging van de Klant (rechtspersoon) blijkt uit het registeruittreksel, de statuten of gelijkwaardige documenten die de identiteit van de Klant (rechtspersoon) aantonen, is een afzonderlijk machtigingsdocument (bijv. een volmacht) niet vereist.

De identificatie van de Beneficial Owner van de Klant

Het Bedrijf moet de Beneficial Owner van de Klant identificeren - een persoon die uiteindelijk eigenaar is van of zeggenschap heeft over de Klant of namens wie een transactie wordt uitgevoerd. Het Bedrijf moet ook maatregelen nemen om de identiteit van de Beneficial Owner te verifiëren, voor zover het Bedrijf er zeker van kan zijn dat het weet wie de Beneficial Owner is. Het Bedrijf kan er niet van uitgaan dat de particulieren zelf de BO's van de Klant zijn, en moet altijd eerst bij de Klant informatie inwinnen over wie de BO is. De identificatie van de BO betekent de identificatie van een natuurlijke persoon of een groep natuurlijke personen. De

Het Bedrijf verzamelt de volgende gegevens over de Beneficial Owner(s) van de Klant:

- naam/namen en achternaam/namen;
- persoonlijk nummer;¹⁴
- burgerschap.¹⁵

Het Bedrijf zal de Klant om informatie vragen over de Beneficial Owner van de Klant (bijv. door de Klant de mogelijkheid te bieden om zijn Beneficial Owner op te geven bij het verzamelen van gegevens over de Klant).

Het Bedrijf brengt de Zakelijke Relatie niet tot stand als de Klant, die een natuurlijke persoon is, een Beneficial Owner heeft die niet dezelfde persoon is als de Klant.

De Beneficial Owner van een juridische entiteit wordt in fasen geïdentificeerd, waarbij de verplichte entiteit doorgaat naar elke volgende fase als de Beneficial Owner van de juridische entiteit niet kan worden vastgesteld in het geval van de vorige fase. De fasen zijn als volgt:

- is het mogelijk om met betrekking tot de Klant die een rechtspersoon is of een persoon die deelneemt aan de transactie, de natuurlijke persoon of personen te identificeren die feitelijk de uiteindelijke zeggenschap hebben over de rechtspersoon of er op enige andere wijze invloed of zeggenschap over uitoefenen, ongeacht de omvang van de aandelen, stemrechten of eigendomsrechten of de directe of indirecte aard ervan;
- of de Klant die een rechtspersoon is of de persoon die deelneemt aan de transactie een natuurlijke persoon of personen heeft die eigenaar is/zijn van of zeggenschap heeft/hebben over de rechtspersoon via direct¹⁶ of indirect¹⁷ aandelenbezit. Hier moet ook rekening worden gehouden met familiebanden en contractuele banden;
- wie de natuurlijke persoon is in het hogere management¹⁸, die moet worden gedefinieerd als de Begunstigde Eigenaar, als gevolg van de uitvoering van de vorige twee fasen het voor de verplichte entiteit niet mogelijk heeft gemaakt om de Begunstigde Eigenaar te identificeren.

De senior manager van de Klant moet alleen in uitzonderlijke gevallen worden aangegeven als de Beneficial Owner, wanneer het Bedrijf alle redelijke inspanningen doet om de Beneficial Owner te bepalen en op voorwaarde dat er geen redenen zijn om te vermoeden dat de identiteit van de Beneficial Owner wordt verborgen. In dit geval moet onder senior manager het hoofd (bijv. CEO) worden verstaan, directeur, hoofd administratie) van de Klant.

¹⁴ in het geval van een buitenlander - geboortedatum (indien beschikbaar - persoonlijk nummer of een andere unieke reeks symbolen die aan die persoon is toegekend, bedoeld voor persoonlijke identificatie);

¹⁵ wanneer een identiteitsdocument geen gegevens over het staatsburgerschap van de klant bevat, moeten financiële instellingen en andere verplichte entiteiten bij het identificeren van de klant die een natuurlijke persoon is in de fysieke aanwezigheid van de klant, de klant vragen om de gegevens over het staatsburgerschap te verstrekken.

¹⁶ **rechtstreeks bezit** is een manier van zeggenschap uitoefenen waarbij de natuurlijke persoon een belang van 25 procent plus één aandeel of een eigendomsrecht van meer dan 25 procent in het bedrijf heeft

¹⁷ **Indirecte eigendom** is een manier van controle uitoefenen waarbij een belang van 25 procent plus één aandeel of een eigendomsrecht van meer dan 25 procent in het bedrijf in handen is van een bedrijf dat gecontroleerd wordt door een natuurlijke persoon of van meerdere bedrijven die gecontroleerd worden door dezelfde natuurlijke persoon.

¹⁸ een **lid van het senior management** is een persoon die de strategische beslissingen neemt die de bedrijfsactiviteiten en/of -praktijken en/of de algemene (bedrijfs)trends van het bedrijf fundamenteel beïnvloeden, of die bij afwezigheid de dagelijkse of gewone managementfuncties van het bedrijf uitvoert binnen het bereik van de uitvoerende macht (bijv. chief executive officer (CEO), chief financial officer (CFO), directeur of president, enz.)

De documenten die worden gebruikt voor de identificatie van de rechtspersoon of de andere ingediende documenten doenniet direct aangeeft wie de Begunstigde Eigenaar van de rechtspersoon is, worden de relevante gegevens (inclusief gegevens over het lid zijn van een groep en de eigendoms- en managementstructuur van de groep) geregistreerd op basis van de verklaring van de vertegenwoordiger van de rechtspersoon of het document dat met de hand geschreven is door de vertegenwoordiger van de rechtspersoon.

Het Bedrijf zal redelijke maatregelen toepassen om de juistheid van de informatie die is vastgesteld op basis van verklaringen of een handgeschreven document te verifiëren (bijv. door navraag te doen in de relevante registers), waarbij overlegging van het jaarverslag van de rechtspersoon of een ander relevant document vereist is. Als het Bedrijf twijfels heeft over de juistheid of volledigheid van de relevante informatie, dan zal het Bedrijf de verstrekte informatie controleren aan de hand van openbaar beschikbare bronnen en, indien nodig, aanvullende informatie opvragen bij de Klant.

Moeilijkheden ondervonden tijdens de Beneficial Owner Identification

Het bedrijf moet zich ervan bewust zijn dat de informatie over uiteindelijke begunstigde eigendom kan worden verdoezeld door het gebruik van lege vennootschappen, complexe eigendoms- en controlestructuren met vele lagen van aandelen geregistreerd op naam van andere rechtspersonen, aandeelhouders en bestuurders op naam, zoals naaste medewerkers en familie, en op andere manieren.

In veel gevallen is de rol van de genomineerde bestuurders en aandeelhouders om de identiteit van de BO en controller van een bedrijf of activa te beschermen of te verbergen. Een nominee kan helpen bij het omzeilen van jurisdictionele controles op bedrijfseigendom en het omzeilen van door rechtbanken en overheidsinstanties opgelegde bestuursverboden. Het bedrijf moet zich dus vooral bewust zijn van de bedrijfsstructuren die de complexiteit bevorderen en het moeilijker maken om nauwkeurige informatie over de uiteindelijke begunstigde te verkrijgen. Verder moet het bedrijf zich bewust zijn van de mogelijkheid dat er nomineeconstructies bestaan waarbij vrienden, familieleden of vennoten beweren de BO's van rechtspersonen, juridische constructies of andere ondernemingen te zijn.

Daarom moet het bedrijf passende en adequate maatregelen nemen om de werkelijke BO's te bepalen en situaties te identificeren waarin de uiteindelijke begunstigde eigenaar wordt verhuuld.

Bij het bepalen van de BO moet het Bedrijf gegevens verzamelen over de eigendomsstructuur van de Klant en deze verifiëren aan de hand van documenten, gegevens of informatie verkregen van een betrouwbare en onafhankelijke bron. In het geval van een Multi-Level Ownership moet het eigendomsstructuurschema worden opgesteld door of verkregen van de Klant.

Het Bedrijf moet er ook voor zorgen dat het de eigendoms- en controlestructuur van de Klant begrijpt, vooral als de eigendoms- en controlestructuur complex is (bijv. de aandeelhouders komen uit verschillende rechtsgebieden; de aandeelhouders zijn van verschillende juridische entiteiten / juridische constructies, er zijn trusts en particuliere beleggingsvehikels binnen de eigendoms- en controlestructuur, de Klant heeft aandelen aan toonder uitgegeven). Het Bedrijf moet beoordelen of de eigendoms- en controlestructuur zinvol is vanuit commercieel, economisch of juridisch oogpunt.

Gebruik van het informatiesysteem van deelnemers aan rechtspersonen

Bij het identificeren van een Begunstigde Eigenaar moet het Bedrijf bovendien gebruik maken van het Informatiesysteem van Deelnemers van Juridische Entiteiten (JADIS) om gegevens te verkrijgen over Begunstigde Eigenaren van de Klant en heeft het recht gebruik te maken van andere staatsinformatiesystemen en registers waarin gegevens over de deelnemers van rechtspersonen worden verzameld. JADIS is toegankelijk via het Lithuanian State Enterprise Centre of Registers (SECR) via de relevante toepassing. De aanvraag kan worden ingediend:

- elektronisch via het [gebruikerszelfbedieningssysteem van het Registratiecentrum](#);
- per e-mail info@registrucentras.lt die ondertekend moet worden met een e-handtekening;
- [bij de klantenservice van het registratiecentrum](#) door het origineel in te dienen.

De voorbereide JADIS-uittreksels en kopieën van documenten kunnen zijn:

- gedownload van de selfservice van het Centrum voor Registers (alleen als de aanvraag via de selfservice van het Centrum voor Registers is ingediend);
- afgehaald bij de klantenservice van het Centrum van Registers;
- per post ontvangen op het door de klant opgegeven adres.

Na vaststelling van de discrepantie tussen de informatie over de Beneficial Owners van de Klant die een rechtspersoon is die beschikbaar is in JADIS en de informatie over de Beneficial Owners van dezelfde klant die voor hen beschikbaar is, de Klant hiervan op de hoogte stellen en voorstellen om nauwkeurige informatie over zijn Beneficial Owners te verstrekken aan de gegevensverwerker van JADIS.

Het Bedrijf zal geen Zakelijke Relatie aangaan of een transactie uitvoeren (met uitzondering van monetaire verrichtingen of transacties die in de loop van een Zakelijke Relatie worden afgesloten en/of uitgevoerd), wanneer de informatie over de Begunstigde Eigenaren van de Klant die een rechtspersoon is, niet in JADIS is verstrekt of wanneer de informatie over de Begunstigde Eigenaren van de Klant die een rechtspersoon is, die in JADIS is verstrekt, onjuist is.

Politieke identificatie van de blootgestelde persoon

Het Bedrijf zal maatregelen nemen om na te gaan of de Klant, de Beneficial Owner van de Klant of de vertegenwoordiger van deze Klant een PEP, hun familielid¹⁹ of naaste medewerker²⁰ is of dat de Klant een dergelijke persoon is geworden.

Het Bedrijf zal de Klant om informatie vragen om vast te stellen of de Klant een PEP, zijn/haar familielid of naaste medewerker is (bijv. door de Klant de mogelijkheid te bieden om de relevante informatie te specificeren bij het verzamelen van gegevens over de Klant).

Het Bedrijf zal de van de Klant ontvangen gegevens verifiëren door navraag te doen in relevante databanken of openbare databanken of door navraag te doen of gegevens te verifiëren op de websites van de relevante toezichthoudende autoriteiten of instellingen van het land waar de Klant zijn woonplaats of zetel heeft. PEP moet bovendien worden geverifieerd met behulp van een internationale zoekmachine (bijv. Google) en de lokale zoekmachine van het land van herkomst van de Klant, indien aanwezig, door de naam van de Klant in te voeren in zowel het Latijnse als het lokale alfabet met de geboortedatum van de Klant.

Daarnaast wordt de screening van de PEP-status geïmplementeerd en uitgevoerd door de geautomatiseerde AML-oplossing Sum & Substance. De oplossing biedt een doorlopende controle van de PEP-status en identificeert familieleden en naaste medewerkers van PEP's.

Ten minste de volgende personen worden als PEP's beschouwd:

- het staatshoofd, het hoofd van de regering, een minister, een vice-minister of een onderminister, een staatssecretaris, een kanselier van het parlement, de regering of een ministerie;
- een lid van het parlement;
- een lid van het Hooggerechtshof, het Constitutioneel Hof of enige andere hoogste gerechtelijke instantie waarvan de beslissingen niet vatbaar zijn voor beroep;
- een burgemeester van de gemeente, een hoofd van de gemeentelijke administratie;
- een lid van het leidinggevend orgaan van de hoogste instelling voor overheidsaudit of -controle, of een voorzitter, vicevoorzitter of lid van de raad van bestuur van de centrale bank;
- ambassadeurs van buitenlandse staten, een zaakgelastigde ad interim, het hoofd van de Litouwse strijdkrachten, commandant van de strijdkrachten en eenheden, chef van de defensiestaf of hoge officier van buitenlandse strijdkrachten;
- een lid van het leidinggevend of toezichthoudend orgaan van een overheidsbedrijf, een naamloze vennootschap of een besloten vennootschap, waarvan de aandelen of een deel van de aandelen, die meer dan 1/2 van het totale aantal stemmen in de algemene vergadering van aandeelhouders van dergelijke bedrijven vertegenwoordigen, in handen zijn van de staat;

¹⁹ **gezinslid**: de echtgeno(o)t(e), de persoon met wie het partnerschap geregistreerd is (d.w.z. de samenwonende), ouders, broers, zussen, kinderen en de echtgeno(o)t(e) van kinderen, samenwonenden van kinderen

²⁰ **naaste medewerker**: een natuurlijke persoon die, samen met PEP, lid is van dezelfde rechtspersoon of van een lichaam zonder rechtspersoonlijkheid of een andere zakelijke relatie onderhoudt; of een natuurlijke persoon die de enige Beneficial Owner is van de rechtspersoon of van een lichaam zonder rechtspersoonlijkheid dat is opgericht of de facto functioneert met als doel eigendom of een ander persoonlijk voordeel voor PEP te verwerven.

- een lid van het bestuurs- of toezichthoudend orgaan van een gemeentelijk bedrijf, een naamloze vennootschap of een besloten vennootschap waarvan de aandelen of een deel van de aandelen, die meer dan 1/2 van het totale aantal stemmen in de algemene vergadering van aandeelhouders van dergelijke bedrijven vertegenwoordigen, in handen zijn van de staat en die worden beschouwd als grote ondernemingen in de zin van de Wet op de jaarrekening van entiteiten van de Republiek Litouwen;
- een directeur, een adjunct-directeur of een lid van het leidinggevend of toezichthoudend orgaan van een internationale intergouvernementele organisatie;
- een leider, een plaatsvervangend leider of een lid van het bestuursorgaan van een politieke partij.

Het bedrijf identificeert naaste medewerkers en familieleden van PEP's alleen als hun connectie met PEP's bekend is bij het publiek of als het bedrijf reden heeft om aan te nemen dat een dergelijke connectie bestaat.

Wanneer een PEP niet langer belast is met een Prominente Publieke Functie, zal het Bedrijf binnen 12 maanden vanaf de datum van uittreding van de PEP uit de publieke functies rekening houden met de risico's die aan de Klant verbonden blijven. Na een periode van 12 maanden vanaf de datum van het aftreden van de PEP uit publieke functies, is het Bedrijf verplicht om de risico's die verbonden zijn aan een dergelijke klant opnieuw te beoordelen.

Identificatie van het doel en de aard van de zakelijke relatie of transactie

Het Bedrijf dient het doel en de aard van het aangaan van de Zakelijke Relatie of het uitvoeren van de transactie te begrijpen. Met betrekking tot de geleverde diensten kan het Bedrijf de Klant om de volgende informatie vragen om het doel en de aard van de Zakelijke Relatie of transactie te begrijpen:

- of de Klant de diensten van het Bedrijf voor zijn eigen behoeften zal gebruiken of de belangen van een andere persoon zal vertegenwoordigen;
- contactinformatie;
- informatie over het geregistreerde adres en het feitelijke woonadres van de Klant;
- de geschatte transactieomzet met het Bedrijf per kalenderjaar;
- de geschatte bron van fondsen die in de Zakelijke relatie of transactie zijn gebruikt;
- of de Zakelijke Relatie of transactie verband houdt met de uitvoering van economische of professionele activiteiten door de Klant en welke activiteiten dat zijn;
- informatie over de bron van fondsen met betrekking tot de Zakelijke relatie of transactie, als het bedrag van de transacties (incl. verwacht bedrag) de vastgestelde limiet overschrijdt.

Het Bedrijf zal aanvullende maatregelen toepassen en aanvullende informatie verzamelen om het doel en de aard van de Zakelijke Relatie vast te stellen in gevallen waarin:

- er sprake is van een situatie die verwijst naar hoge waarde of ongebruikelijk is en/of
- wanneer het risico en/of risicoprofiel verbonden aan de Klant en de aard van de Zakelijke Relatie aanleiding geeft tot het uitvoeren van aanvullende acties om de Zakelijke Relatie adequaat te kunnen monitoren.

Als de Klant een rechtspersoon is, zal het Bedrijf, naast het bovengenoemde, het **werkkerrein van** de Klant identificeren, waarbij het Bedrijf zal begrijpen waarmee de Klant zich bezighoudt en van plan is zich bezig te houden in de loop van de Zakelijke Relatie en hoe dit overeenkomt met het doel en de aard van de Zakelijke Relatie in het algemeen en of dit redelijk, begrijpelijk en aannemelijk is.

Het activiteitengebied moet passen in het ervaringsprofiel van de vertegenwoordiger (of sleutelfiguren) van de Klant en/of de Beneficial Owner. Het Bedrijf moet dus vaststellen waar de capaciteit, bekwaamheid, vaardigheden en kennis (ervaring in het algemeen) van de vertegenwoordiger en/of de Beneficial Owner vandaan komen om in dit activiteitengebied, met deze bedrijfsvolumes en met deze belangrijkste zakelijke partners te werken.

Bewaking van de zakenrelatie

Het Bedrijf houdt toezicht op gevestigde Zakelijke Relaties waar de volgende voortdurende due diligence (periodieke) maatregelen worden geïmplementeerd:

- ervoor zorgen dat de documenten, gegevens of informatie die tijdens de toepassing van due diligence-maatregelen worden verzameld, regelmatig en in het geval van triggervoorvallen worden bijgewerkt, d.w.z. in de eerste plaats de gegevens over de Klant, zijn vertegenwoordiger (inclusief het recht van vertegenwoordiging) en Beneficial Owner, evenals het doel en de aard van de Zakelijke Relatie;
- voortdurende controle van de Zakelijke Relatie, die betrekking heeft op transacties die in het kader van de zakelijke relatie worden uitgevoerd om ervoor te zorgen dat de transacties overeenkomen met de kennis van het Bedrijf over de Klant, zijn activiteiten en zijn risicoprofiel;
- identificatie van de bron en herkomst van fondsen die gebruikt zijn in de transactie(s).

De onderneming **controleert en actualiseert** regelmatig **de documenten, gegevens en informatie** die tijdens de uitvoering van CDD-maatregelen zijn verzameld en werkt het risicoprofiel van de cliënt bij. De regelmaat van de controles en updates moet gebaseerd zijn op het risicoprofiel van de Klant en de controles moeten ten minste plaatsvinden:

- eenmaal per half jaar voor Klanten met een hoog risicoprofiel;
- eenmaal per jaar voor de Klant met een gemiddeld risicoprofiel;
- eens in de twee jaar voor het laagrisicoprofiel Klant.

Het Bedrijf heeft een systeem geïmplementeerd voor het opslaan, systematiseren en controleren van de documenten van de Klant. Het systeem stelt de verantwoordelijke medewerker automatisch op de hoogte van de noodzaak om een actueel document op te vragen in overeenstemming met het risicoprofiel van de Klant. Het systeem controleert ook de vervaldatum en stuurt een melding als het ID-document/Adresbewijs van de Klant bijna verlopen is.

De verzamelde documenten, gegevens en informatie moeten ook gecontroleerd worden als er een gebeurtenis heeft plaatsgevonden die aangeeft dat de verzamelde documenten, gegevens en informatie bijgewerkt moeten worden.

In het kader van de **voortdurende controle van de Zakelijke Relatie** controleert het Bedrijf de transacties die tijdens de Zakelijke Relatie worden gesloten op zodanige wijze dat het Bedrijf kan vaststellen of de te sluiten transacties overeenstemmen met de informatie die eerder over de Klant bekend was (d.w.z. wat de Klant bij het aangaan van de Zakelijke Relatie heeft verklaard of wat in de loop van de Zakelijke Relatie bekend is geworden).

Het Bedrijf zal de Zakelijke Relatie ook controleren om de activiteiten of feiten van de Klant vast te stellen die duiden op criminele activiteiten, het witwassen van geld of de financiering van terrorisme of waarvan het verband met het witwassen van geld of de financiering van terrorisme waarschijnlijk is, met inbegrip van gecompliceerde, waardevolle en ongebruikelijke transacties en transactiepatronen die geen redelijk of duidelijk economisch of legitiem doel hebben of die niet kenmerkend zijn voor de specifieke kenmerken van het bedrijf in kwestie. In de loop van de Zakelijke Relatie beoordeelt het Bedrijf voortdurend de veranderingen in de activiteiten van de Klant en beoordelen of deze veranderingen het risiconiveau van de Klant en de Zakelijke Relatie kunnen verhogen, waardoor het nodig wordt om EDD-maatregelen toe te passen.

In het kader van de voortdurende controle van de Zakenrelatie past het Bedrijf de volgende maatregelen toe:

- screening, d.w.z. het bewaken van transacties in realtime;
- monitoring, d.w.z. het later analyseren van

transacties. Het doel van **screening** is om te identificeren:

- verdachte en ongebruikelijke transacties en transactiepatronen;
- transacties die de voorziene drempels overschrijden;
- politiek prominente personen en omstandigheden met betrekking tot sancties.

De screening van de transacties wordt automatisch uitgevoerd en omvat de volgende maatregelen:

- vastgestelde drempels voor de transacties van de Klant, afhankelijk van het risicoprofiel van de Klant en de geschatte transactieomzet die door de Klant is opgegeven;
- het scoren van Virtual Currency wallets waar de Virtual Currency naartoe worden gestuurd in overeenstemming met de bestelling van de Klant;
- het scoren van Virtuele Valutawallets waarvan de Virtuele Valuta wordt ontvangen.

Als de Klant opdracht geeft voor een transactie die de vastgestelde drempel overschrijdt of voor een transactie naar een portemonnee voor virtuele valuta met een hoge risicoscore (bijv. portemonnees die gerelateerd zijn aan fraude, misdaad, etc.), wordt de transactie handmatig goedgekeurd door de Medewerker, die voor de goedkeuring beoordeelt of het nodig is om aanvullende CDD-maatregelen toe te passen (bijv. het toepassen van EDD-maatregelen, het vragen naar de bron en herkomst van fondsen of het vragen naar aanvullende informatie over de transactie).

Bij het **controleren van transacties** beoordeelt de Werknemer de transactie met het oog op het opsporen van activiteiten en transacties die:

- afwijken van wat redelijkerwijs verwacht mag worden op basis van de uitgevoerde CDD-maatregelen, de verleende diensten, de door de Klant verstrekte informatie en andere omstandigheden (bijv. overschrijding van de geschatte transactieomzet, Virtuele Valuta die telkens naar een nieuwe Virtuele Valutawallet wordt verzonden, transactievolume dat de limiet overschrijdt); zonder af te wijken van de vorige clausule, mag worden verondersteld deel uit te maken van een witwasoperatie of terrorismefinanciering;
- kan van invloed zijn op de score van het risicoprofiel van de Klant.

In het geval dat het bovengenoemde feit wordt ontdekt, zal de Werknemer MLRO hiervan op de hoogte stellen en elke transactie van de Klant uitstellen totdat MLRO hierover een besluit heeft genomen.

In aanvulling op het bovenstaande zal de MLRO regelmatig (ten minste eenmaal per week) de transacties van het bedrijf controleren om ervoor te zorgen dat:

- de Werknemers van het Bedrijf de bovengenoemde verplichtingen naar behoren hebben uitgevoerd;
- er zijn geen transacties en transactiepatronen die ingewikkeld, waardevol en ongebruikelijk zijn en die geen redelijk of duidelijk economisch of legitiem doel hebben of die niet kenmerkend zijn voor de specifieke kenmerken.

Het Bedrijf **identificeert** indien nodig **de bron²¹ en oorsprong²² van de fondsen** die in transactie(s) worden gebruikt. De noodzaak om de bron en herkomst van fondsen te identificeren hangt af van de eerdere activiteiten van de Klant en andere bekende informatie. Daarbij zal de identificatie van de bron en herkomst van de fondsen die in de transactie gebruikt worden in de volgende gevallen uitgevoerd worden:

- de transacties de door het Bedrijf vastgestelde limieten overschrijden;
- de transacties komen niet overeen met de informatie die eerder over de Klant bekend was;
- het Bedrijf het nodig wil of redelijkerwijs nodig moet achten om te beoordelen of de transacties overeenkomen met de informatie die eerder over de Klant bekend was;
- het bedrijf vermoedt dat de transacties wijzen op criminele activiteiten, het witwassen van geld of de financiering van terrorisme of dat het verband tussen de transacties en het witwassen van geld of de financiering van terrorisme waarschijnlijk is, incl. gecompliceerde, waardevolle en ongebruikelijke transacties en transactiepatronen die geen redelijk of duidelijk economisch of legitiem doel hebben of die niet kenmerkend zijn voor de specifieke kenmerken van het bedrijf in kwestie.

UITVOERING VAN SANCTIES

Bij de inwerkingtreding, wijziging of beëindiging van Sancties zal de Vennootschap verifiëren of de Klant, zijn Beneficial Owner of een persoon die van plan is de Zakelijke Relatie of transactie met hem aan te gaan, onderworpen is aan Sancties. Als het Bedrijf een persoon identificeert die onderhevig is aan Sancties of als de door hen voorgenomen of uitgevoerde transactie in strijd is met Sancties, past het Bedrijf Sancties toe en informeert het FCIS hierover binnen 3 uur.

Procedure voor het identificeren van het onderwerp van sancties en een transactie die sancties schendt

Het Bedrijf gebruikt ten minste de volgende bronnen (databases) om de relatie van de Klant met Sancties te verifiëren:

- [Een geconsolideerde lijst van EU-sancties;](#)
- [Een geconsolideerde lijst van sancties van de Verenigde Naties](#)
- [Bureau voor controle op buitenlandse activa \(OFAC\).](#)

Naast bovengenoemde bronnen kan het bedrijf andere bronnen gebruiken op besluit van de

werknemer die CDD-maatregelen toepast.

²¹ **de bron van de fondsen** die gebruikt zijn in de transactie is reden, uitleg en basis (rechtsverhouding en de inhoud daarvan) waarom de fondsen werden overgemaakt

²² **de oorsprong van de fondsen** die gebruikt zijn in de transactie is de activiteit waarmee de fondsen verdiend of ontvangen zijn

Om te verifiëren dat de namen van de personen die uit het onderzoek naar voren komen, dezelfde zijn als de personen die in een kennisgeving met sanctie(s) worden vermeld, worden hun persoonsgegevens gebruikt, waarvan de belangrijkste kenmerken voor een rechtspersoon de naam of het handelsmerk, de registratiecode of registratiedatum zijn, en voor een natuurlijke persoon de naam en persoonlijke identificatie of geboortedatum.

Om de identiteit vast te stellen van de personen die in de relevante wettelijke handeling of kennisgeving worden genoemd en die dezelfde zijn als de personen die zijn geïdentificeerd als resultaat van het onderzoek uit databases, moet het Bedrijf de namen van de personen die zijn gevonden als resultaat van het onderzoek analyseren op basis van het mogelijke effect van factoren die persoonsgegevens vervormen (bijv. transcriptie van buitenlandse namen, andere volgorde van woorden, vervanging van diakritische tekens of dubbele letters, enz.)

Het Bedrijf voert bovengenoemde verificaties doorlopend uit in de loop van een gevestigde Zakelijke Relatie. De frequentie van de doorlopende verificaties hangt af van het risicoprofiel van de Klant:

- eenmaal per week voor het hoogrisicoprofiel Klant;
- één keer per maand voor de Klant met een gemiddeld risicoprofiel;
- eenmaal per kwartaal voor de Klant met een laag risicoprofiel.

Als de Werknemer twijfelt of een persoon het onderwerp is van Sancties, stelt de Werknemer de MLRO of het directielid hiervan onmiddellijk op de hoogte. In dit geval beslist de MLRO of het directielid of hij/zij aanvullende gegevens van de persoon vraagt of verkrijgt, of dat hij/zij het FCIS onmiddellijk op de hoogte stelt van zijn/haar vermoeden.

Het Bedrijf zal in de eerste plaats zelf aanvullende informatie inwinnen over de persoon die een Zakelijke Relatie heeft of een transactie met hen uitvoert, evenals over de persoon die van plan is een Zakelijke Relatie aan te gaan, een transactie of een handeling met hen te verrichten, waarbij de voorkeur wordt gegeven aan informatie uit een geloofwaardige en onafhankelijke bron. Als dergelijke informatie om de een of andere reden niet beschikbaar is, zal het Bedrijf de persoon die een Zakelijke Relatie heeft of een transactie of handeling met hen verricht, evenals de persoon die van plan is een Zakelijke Relatie aan te gaan, een transactie of handeling met hen te verrichten, vragen of de informatie afkomstig is van een geloofwaardige en onafhankelijke bron en het antwoord beoordelen.

Acties bij het identificeren van het Sanctieonderwerp of een transactie die Sancties schendt

Als de Medewerker van het Bedrijf zich ervan bewust wordt dat de Klant die een Zakelijke Relatie onderhoudt of een transactie uitvoert met het Bedrijf, evenals een persoon die van plan is een Zakelijke Relatie aan te gaan of een transactie uit te voeren met het Bedrijf, het onderwerp is van Sancties, stelt de Medewerker de MLRO of het lid van de Raad van Bestuur onmiddellijk op de hoogte van de identificatie van het onderwerp van Sancties, van de twijfel daarover en van de genomen maatregelen.

De MLRO of het lid van de raad van bestuur weigert een transactie of procedure af te sluiten, neemt de maatregelen waarin het besluit betreffende het opleggen of uitvoeren van de sancties voorziet en stelt het FCIS onmiddellijk in kennis van zijn twijfels en van de genomen maatregelen.

Bij het identificeren van het onderwerp van de sancties is het noodzakelijk om de maatregelen te identificeren die genomen worden om deze persoon te sanctioneren. Deze maatregelen worden beschreven in de rechtshandeling die de

Sancties, daarom is het noodzakelijk om de exacte sanctie vast te stellen die tegen de persoon wordt uitgevoerd om ervoor te zorgen dat de maatregelen legaal en correct worden toegepast.

WEIGERING VAN DE TRANSACTIE OF ZAKELIJKE RELATIE EN HUN BEËINDIGING

Het is het Bedrijf verboden om een Zakelijke Relatie aan te gaan en de aangegane Zakelijke Relatie of transactie zal worden beëindigd (tenzij dit objectief gezien onmogelijk is) in het geval dat:

- het Bedrijf vermoedt dat er sprake is van het witwassen van geld of de financiering van terrorisme;
- het voor het Bedrijf onmogelijk is om de CDD-maatregelen toe te passen, omdat de Klant de relevante gegevens niet indient of weigert in te dienen, of de ingediende gegevens geen reden geven om er zeker van te zijn dat de verzamelde gegevens toereikend zijn;
- de Klant waarvan het kapitaal bestaat uit aandelen aan toonder of andere effecten aan toonder wil de Zakelijke Relatie aangaan;
- de Klant die een natuurlijke persoon is achter wie een andere, feitelijk begunstigde persoon staat, wil de Zakelijke Relatie aangaan (vermoeden dat een persoon die als dekmantel fungeert wordt gebruikt);
- het risicoprofiel van de Klant is niet meer in overeenstemming met de risicobereidheid van het Bedrijf (d. w. z. het risicoprofielniveau van de Klant is "verboden").

In het geval van een beëindiging van de Zakelijke Relatie in overeenstemming met dit hoofdstuk, zal het Bedrijf de tegoeden van de Klant binnen een redelijke termijn, maar bij voorkeur niet later dan binnen een maand na de beëindiging en in hun geheel, overmaken naar een rekening bij een kredietinstelling die geregistreerd is of waarvan de vestiging zich bevindt in een verdragsluitende staat van de Europese Economische Ruimte of in een land waar vereisten gelden die gelijk zijn aan die in de relevante richtlijnen van het Europees Parlement en de Raad. In uitzonderlijke gevallen kunnen activa naar een andere rekening dan die van de Klant worden overgeboekt of in contanten worden uitgegeven. Ongeacht de ontvanger van de tegoeden is de minimale informatie die in het Engels in de betalingsgegevens van de overboeking van de tegoeden van de Klant wordt vermeld, dat de overboeking verband houdt met de buitengewone beëindiging van de relatie met de Klant.

RAPPORTAGE VERPLICHTING

Het bedrijf moet de transactie opschorten, ongeacht het bedrag van de transactie (behalve in de gevallen waarin dit objectief onmogelijk is vanwege de aard van de monetaire verrichting of transactie, de wijze van uitvoering ervan of andere omstandigheden) en moet via zijn MLRO verslag uitbrengen aan het FCIS over de activiteit of de omstandigheden die zij vaststellen in de loop van economische activiteiten en waarbij:

- het Bedrijf heeft vastgesteld dat de Klant een verdachte transactie uitvoert;

- het Bedrijf weet of vermoedt dat activa van enige waarde direct of indirect zijn verkregen uit criminele activiteiten of deelname aan dergelijke activiteiten.

De minimale kenmerken van verdachte transacties staan in de richtlijnen van het FCIS (een van de bijlagen van deze richtlijnen).

De hierboven vermelde meldingen moeten vóór de voltooiing van de transactie worden gedaan als het bedrijf vermoedt of weet dat er sprake is van het witwassen van geld of de financiering van terrorisme of aanverwante misdrijven en als deze omstandigheden vóór de voltooiing van de transactie worden vastgesteld.

Als de noodzaak van bovengenoemd rapport zich voordoet, moet de Werknemer aan wie een dergelijke noodzaak bekend is geworden, de MLRO hiervan onmiddellijk op de hoogte stellen.

In elk geval (d.w.z. ook in de situatie waarin een activiteit of omstandigheid wordt geïdentificeerd nadat de transactie is voltooid) **moet de meldingsplicht voor de bovenstaande meldingen onmiddellijk worden uitgevoerd, maar niet later dan drie werkuren** na de identificatie van de activiteit of omstandigheid of het ontstaan van het feitelijke vermoeden (d.w.z. de situatie waarin het vermoeden niet kan worden weggenomen).

Rapportageverplichting met betrekking tot specifieke soorten transacties

Het Bedrijf moet via zijn MLRO uiterlijk binnen 7 werkdagen na de identificatie van wisseltransacties in Virtuele Valuta of transacties in Virtuele Valuta informatie naar het FCIS sturen, als de dagelijkse waarde van dergelijke transactie(s) gelijk is aan of hoger is dan EUR 15.000 of het equivalente bedrag in vreemde of Virtuele Valuta, ongeacht of de transactie is afgesloten in een of meer gerelateerde monetaire transacties.

In het hierboven gespecificeerde geval moet de bij FCIS ingediende informatie het volgende omvatten:

- de gegevens die de identiteit van de Klant bevestigen, en wanneer de transactie via een vertegenwoordiger wordt uitgevoerd - ook de gegevens die de identiteit van de vertegenwoordiger bevestigen;
- het bedrag van de transactie;
- de valuta waarin de transactie is uitgevoerd;
- de datum van uitvoering van de transactie;
- de wijze van uitvoering van de monetaire transactie;
- de entiteit ten gunste van wie de monetaire transactie werd uitgevoerd (indien mogelijk);
- andere gegevens die in de relevante FCIS-instructies worden gespecificeerd.

Alle rapporten die in dit hoofdstuk worden beschreven, moeten worden verzonden in overeenstemming met de rapportagerichtlijnen van het Bedrijf via een beveiligd kanaal dat volledige vertrouwelijkheid garandeert (een van de bijlagen van deze Richtlijnen).

Het is het Bedrijf, een structurele eenheid van het Bedrijf, een lid van de Raad van Bestuur, MLRO en de Werknemer verboden om een persoon, zijn Beneficial Owner, vertegenwoordiger of derde partij te informeren over een rapport dat over hen is ingediend bij het FCIS, een plan om een dergelijk rapport in te dienen of het optreden van

van de melding, maar ook over een voorschrift van het FCIS of over het begin van een strafprocedure.

TRAININGSVERPLICHTING

Het Bedrijf zorgt ervoor dat haar Werknemers, aannemers en anderen die op vergelijkbare basis deelnemen aan het bedrijf en die werktaken uitvoeren die van belang zijn voor het voorkomen van het gebruik van het bedrijf van het Bedrijf voor het witwassen van geld of de financiering van terrorisme ("Relevante Personen") de relevante kwalificaties hebben voor deze werktaken. Wanneer een Relevant Persoon wordt aangeworven of in dienst genomen, worden de kwalificaties van de Relevante Persoon gecontroleerd als onderdeel van het aanwervings-/benoemingsproces door het uitvoeren van achtergrondcontroles, die worden gedocumenteerd met behulp van een speciaal standaardformulier dat de geschiktheid van werknemers beoordeelt.

In overeenstemming met de vereisten die van toepassing zijn op de Vennootschap met betrekking tot het waarborgen van de geschiktheid van Relevante Personen, zorgt de Vennootschap ervoor dat dergelijke personen doorlopend passende training en informatie ontvangen om de verplichtingen van de Vennootschap in overeenstemming met de toepasselijke wetgeving te kunnen vervullen. Door middel van training wordt ervoor gezorgd dat dergelijke personen voldoende kennis hebben op het gebied van AML/CFT, rekening houdend met de taken en functie van de persoon in kwestie. De training moet in de eerste plaats informatie verschaffen over de meest moderne methoden voor het witwassen van geld en de financiering van terrorisme en de risico's die daaruit voortvloeien.

Deze training verwijst naar relevante delen van de inhoud van de toepasselijke regels en voorschriften, de risicobeoordeling van de Onderneming, de Richtlijnen en procedures van de Onderneming en informatie die het voor deze Relevante Personen gemakkelijker moet maken om vermoedens van Witwassen en Terrorismefinanciering op te sporen. De training is gestructureerd op basis van de risico's die door middel van het risicobeoordelingsbeleid zijn geïdentificeerd.

De inhoud en frequentie van de training wordt aangepast aan de taken en functie van de persoon met betrekking tot kwesties die verband houden met AML/CFT-maatregelen. Als de richtlijnen op de een of andere manier bijgewerkt of gewijzigd worden, worden de inhoud en frequentie van de training dienovereenkomstig aangepast.

Voor nieuwe Werknemers omvat de training een overzicht van de inhoud van de toepasselijke regels en voorschriften, het risicobeoordelingsbeleid van het Bedrijf, deze Richtlijnen en andere relevante procedures.

De werknemers en de leden van de Raad van Bestuur krijgen doorlopend training onder auspiciën van de MLRO in overeenstemming met het volgende trainingsplan:

- Periodiciteit: minstens één keer per jaar voor de leden van de Raad van Bestuur. Ten minste eenmaal per jaar voor de Werknemers van het Bedrijf en de Betrokkene.
- reikwijdte: beoordeling van toepasselijke regels en voorschriften, de Richtlijnen van het Bedrijf en andere relevante procedures. Specifieke informatie met betrekking tot nieuwe/geactualiseerde kenmerken in de toepasselijke regels en voorschriften. Verslag en uitwisseling van ervaringen met betrekking tot transacties die sinds de vorige training zijn beoordeeld.

Naast het bovenstaande worden Relevante Personen voortdurend op de hoogte gehouden van nieuwe trends, patronen en methoden en worden zij voorzien van andere informatie die relevant is voor de preventie van het witwassen van geld en de financiering van terrorisme. De gegeven training moet elektronisch worden gedocumenteerd en bevestigd met de handtekening van de relevante persoon. Deze documentatie moet de inhoud van de training, de namen van de deelnemers en de datum van de training bevatten.

VERZAMELEN EN OPSLAAN VAN GEGEVENS, LOGBOEKEN

Het Bedrijf zal via de persoon (inclusief werknemers, leden van de Raad van Bestuur en MLRO) die als eerste de relevante informatie of documenten ontvangt, de volgende gegevens registreren en bewaren:

- alle verzamelde gegevens binnen de implementatie van CDD-maatregelen;
- informatie over de omstandigheden van weigering van het aangaan van de Zakelijke Relatie door het Bedrijf;
- de omstandigheden van de weigering om een Zakelijke Relatie aan te gaan op initiatief van de Klant als de weigering verband houdt met de toepassing van CDD-maatregelen door het Bedrijf;
- informatie over alle verrichtingen om de persoon die aan de transactie deelneemt of de Begunstigde Eigenaar van de Klant te identificeren;
- informatie als het onmogelijk is om de CDD -maatregelen uit te voeren;
- informatie over de omstandigheden van beëindiging van de zakelijke relatie in verband met de onmogelijkheid om de CDD-maatregelen toe te passen
- de datum of periode van elke transactie en een beschrijving van de inhoud van de transactie, inclusief het transactiebedrag, de valuta en het rekeningnummer of een andere identificatiecode (incl. hash van transacties in Virtuele Valuta en Virtuele Valutawallets met betrekking tot de transactie);
- informatie die als basis dient voor de rapportageverplichtingen zoals gespecificeerd in de Richtlijnen;
- gegevens over verdachte of ongebruikelijke transacties of omstandigheden waarvan het FCIS niet op de hoogte werd gebracht (bijv. complexe of ongebruikelijk grote transacties, transacties volgens een ongebruikelijk patroon en transacties die geen duidelijk economisch of rechtmatig doel hebben, zakelijke relaties of monetaire transacties met klanten uit derde landen waar de maatregelen ter voorkoming van het witwassen van geld en/of de financiering van terrorisme ontoereikend zijn of niet voldoen aan de internationale normen volgens informatie die officieel gepubliceerd is door internationale intergouvernementele organisaties).

Sommige van de hierboven gespecificeerde gegevens worden in chronologische volgorde in het logboek (zoals hieronder beschreven) ingevoerd op basis van documenten die een monetaire transactie bevestigen of andere rechtsgeldige documenten in verband met de uitvoering van monetaire transacties, onmiddellijk, maar niet later dan binnen 3 werkdagen na de uitvoering van een monetaire transactie.

De hierboven gespecificeerde gegevens moeten 8 jaar na het einde van de zakelijke relatie of de voltooiingstransactie worden bewaard. De gegevens met betrekking tot de uitvoering van de rapportageverplichting moeten tot 5 jaar na de uitvoering van de rapportageverplichting worden bewaard.

De correspondentie van een Zakelijke Relatie met de Klant moet 5 jaar bewaard worden vanaf de datum van beëindiging van de transacties of Zakelijke Relatie.

Documenten en gegevens moeten zo worden bewaard dat er een uitputtend en onmiddellijk antwoord kan worden gegeven op vragen van het FCIS of, krachtens de wetgeving, van andere toezichthoudende autoriteiten, onderzoeksautoriteiten of de rechtbank.

Het bedrijf implementeert alle regels voor de bescherming van persoonsgegevens bij toepassing van de vereisten die voortvloeien uit de toepasselijke wetgeving. Het bedrijf mag persoonlijke gegevens die verzameld zijn bij de CDD-implementatie, alleen verwerken ter voorkoming van het witwassen van geld en de financiering van terrorisme en de gegevens mogen niet verder verwerkt worden op een manier die niet aan het doel voldoet, bijvoorbeeld voor marketingdoeleinden.

Het Bedrijf verwijdert de bewaarde gegevens na het verstrijken van de termijn, tenzij de wetgeving die het betreffende gebied regelt een andere procedure voorschrijft. Op basis van een voorschrift van de bevoegde toezichthoudende autoriteit mogen gegevens die van belang zijn voor het voorkomen, opsporen of onderzoeken van het witwassen van geld of de financiering van terrorisme langer bewaard worden, maar niet langer dan twee jaar na het verstrijken van de eerste termijn.

Registratie logboeken bijhouden

Met het oog op het nakomen van de AML-verplichtingen moet het Bedrijf de volgende registratielogboeken bijhouden (invullen) die de Monetaire Verrichtingen en transacties weergeven (hierna - logboeken):

- logboek van klanten die transactie(s) in Virtuele Valuta uitvoeren, ongeacht of de transactie(s) occasioneel of in de loop van een Zakelijke Relatie worden uitgevoerd;
- logboek van monetaire verrichtingen of transacties tussen de Klant en het Bedrijf voorafgaand aan het moment waarop het Bedrijf verplicht is om CDD-maatregelen toe te passen;
- logboek van meldingen²³ en verdachte geldtransacties en -transacties;
- logboek van de Klanten met wie transacties of Zakelijke Relaties werden geweigerd of beëindigd onder de omstandigheden die verband houden met schendingen van de procedure ter voorkoming van het witwassen van geld en/of de financiering van terrorisme.

Het registratielogboek van Klanten die transacties in Virtuele Valuta uitvoeren, bevat het volgende:

- gegevens die de identiteit van de Klant en zijn vertegenwoordiger bevestigen (als de monetaire transactie wordt uitgevoerd of de transactie wordt afgesloten via een vertegenwoordiger): naam en achternaam van een natuurlijk persoon, persoonlijke identificatiecode (geboortedatum van een buitenlandse Klant), nationaliteit; persoonlijke code, als een dergelijke code wordt verstrekt;
- in het geval van transacties of transacties in virtuele valuta is het niet objectief mogelijk om de begunstigde te identificeren, andere informatie waarmee het adres van de virtuele valuta kan worden geïdentificeerd.

²³ zoals beschreven in het betreffende hoofdstuk van deze Richtlijnen

gekoppeld aan de identiteit van de eigenaar van de virtuele valuta: Internet Protocol (IP)-adres, e-mailadres, enz;

- Adres(sen) van virtuele valuta met betrekking tot transactie en hash(s) van transactie;
- transactiemethode: storting of opname van Virtuele Valuta, Virtuele Valuta wordt omgewisseld naar geld of omgekeerd, Virtuele Valuta wordt omgewisseld naar andere Virtuele Valuta, Virtuele Valuta wisseltransactie werd bemiddeld (p2p uitwisseling);

Het registratielogboek van monetaire verrichtingen of transacties die tussen de cliënt en het bedrijf zijn uitgevoerd voordat het bedrijf verplicht is CDD-maatregelen toe te passen, bevat het volgende:

- gegevens die de identiteit van de Klant en zijn vertegenwoordiger bevestigen (als de monetaire transactie wordt uitgevoerd of de transactie wordt afgesloten via een vertegenwoordiger): naam en achternaam van een natuurlijk persoon, persoonlijke identificatiecode (geboortedatum van een buitenlandse Klant), nationaliteit; persoonlijke code, als een dergelijke code wordt verstrekt;
- gegevens over de monetaire transactie of de transactie: de datum van de transactie, beschrijving van de activa waarop de transactie betrekking heeft (contant geld, onroerend goed, virtuele valuta, enz.) en de waarde ervan (geldbedrag, valuta waarin de monetaire transactie of de transactie wordt uitgevoerd, marktwaarde van de activa, enz.);
- transactiemethode: Virtuele Valuta wordt omgewisseld in geld of omgekeerd, de Klant heeft vooruitbetaald voor het kopen van Virtuele Valuta, enz.

Het registratielogboek van meldingen, verdachte monetaire transacties en transacties bevat het volgende in chronologische volgorde:

- gegevens die de identiteit van de Klant en zijn vertegenwoordiger bevestigen (als de monetaire transactie wordt uitgevoerd of de transactie wordt afgesloten via een vertegenwoordiger): naam en achternaam van een natuurlijk persoon, persoonlijke identificatiecode (geboortedatum van een buitenlandse Klant), nationaliteit; persoonlijke code, als een dergelijke code wordt verstrekt;
- het door het Ministerie van Binnenlandse Zaken van de Republiek Litouwen goedgekeurde criterium, op grond waarvan wordt erkend dat de monetaire transactie of de transactie van de Klant als verdacht wordt beschouwd, de transactie of de transactie voldoet aan;
- Wijze van uitvoering van verdachte monetaire transactie;
- Datum en tijd van de verdachte monetaire transactie, aard van de activa waarop de transactie betrekking heeft (contanten, enz.), en de waarde ervan (geldbedrag, valuta gebruikt voor de uitvoering van de monetaire transactie, marktwaarde van de activa);
- de gegevens over de begunstigde(n) van de transactie: volledige naam en persoonlijk identificatienummer van een natuurlijke persoon (in het geval van een buitenlander: geboortedatum, indien beschikbaar, persoonlijk identificatienummer of een andere unieke reeks symbolen die aan de desbetreffende persoon is toegewezen voor persoonlijke identificatie), en in het geval van een rechtspersoon, titel, rechtsvorm, geregistreerd adres en registratienummer, indien dit is toegewezen;

- Contactgegevens van de Klant: telefoonnummer(s), e-mailadres(sen), contactperso(n)en(en), hun telefoonnummers, e-mailadressen, enz;
- Beschrijving van activa die de Klant niet kan controleren of gebruiken vanaf het moment van opschorting van de verdachte monetaire transactie of transactie (plaats en andere informatie die de activa kenmerkt);
- In het geval van een verdachte monetaire transactie of transactie niet is opgeschort, relevante redenen;
- Methoden voor accountbeheer;
- Andere relevante details, volgens de beslissing van de Werknemer.

Het Bedrijf zal in het registratielogboek van klanten, waar transacties of Zakelijke Relaties zijn beëindigd, het volgende opnemen, in chronologische volgorde:

- gegevens die de identiteit van de Klant en zijn vertegenwoordiger bevestigen (als de monetaire transactie wordt uitgevoerd of de transactie wordt afgesloten via een vertegenwoordiger): naam en achternaam van een natuurlijk persoon, persoonlijke identificatiecode (geboortedatum van een buitenlandse Klant), nationaliteit; persoonlijke code, als een dergelijke code wordt verstrekt;
- gegevens over de monetaire transactie of de transactie: de datum van de transactie, beschrijving van de activa waarop de transactie betrekking heeft (contant geld, onroerend goed, virtuele valuta, enz.) en de waarde ervan (geldbedrag, valuta waarin de monetaire transactie of de transactie wordt uitgevoerd, marktwaarde van de activa, enz;)
- in het geval van transacties of transacties in virtuele valuta waarbij het niet objectief mogelijk is om de begunstigde te identificeren, andere informatie waarmee het adres van de virtuele valuta kan worden gekoppeld aan de identiteit van de eigenaar van de virtuele valuta: internetprotocoladres (IP-adres), e-mailadres, enz;
- in het geval van transacties in virtuele valuta het/de adres(sen) van de virtuele valuta die verband houden met de transactie en de hash(s) van de transactie;
- de gegevens over de begunstigde(n) van de Klant: volledige naam en persoonlijk identificatienummer van een natuurlijke persoon (in het geval van een buitenlander: geboortedatum, indien beschikbaar, persoonlijk identificatienummer of een andere unieke reeks symbolen die aan de desbetreffende persoon is toegewezen voor persoonlijke identificatie), en in het geval van een rechtspersoon, titel, rechtsvorm, geregistreerd adres en registratienummer, indien dit is toegewezen;
- Redenen voor beëindiging van transacties of zakenrelaties in verband met overtredingen van de procedure ter voorkoming van het witwassen van geld en/of de financiering van terrorisme.

Procedure voor het bijhouden en beheren van registratielogboeken

Als het lid van de raad van bestuur op zakenreis is, of om andere geldige redenen niet beschikbaar is, wordt de opslag van loggegevens aangevuld en op een elektronisch medium bewaard door een andere Werknemer, zoals aangegeven in de speciale opdracht van de directeur, waarin de reikwijdte van de taken en verantwoordelijkheden worden uiteengezet die worden toegewezen aan een persoon die als vervanger optreedt.

De raad van bestuur benoemt een medewerker die tot taak heeft de gegevens in de registratielogboeken, die op een elektronisch medium worden verwerkt, te beschermen tegen ongeoorloofde verwijdering, wijziging of gebruik door onbevoegde derden.

De details moeten worden opgeslagen met behulp van software waarmee de details kunnen worden geëxporteerd naar Microsoft Office Excel, Word of gelijkwaardige open-code software, zonder dat de integriteit van de details wordt aangetast.

Het bijhouden van de registratielogboeken wordt gecontroleerd door een lid van de raad van bestuur, als hij/zij op zakenreis is, of om andere geldige redenen niet beschikbaar is, een andere verantwoordelijke Werknemer die door het Bedrijf is aangesteld, zoals aangegeven in de speciale order van de directeur, waarin de reikwijdte van de taken en verantwoordelijkheden worden uiteengezet die zijn toegewezen aan een persoon die als vervanger optreedt.

Het is de Werknemers van het Bedrijf verboden om een Klant of andere personen te informeren of anderszins te laten weten dat informatie over de Geldverrichtingen die plaatsvinden, of transacties die door een Klant worden uitgevoerd, of het daaruit voortvloeiende onderzoek aan het FCIS wordt doorgegeven.

INTERNE CONTROLE OP DE UITVOERING VAN DE RICHTLIJNEN

De uitvoering van de Richtlijnen wordt intern gecontroleerd door het lid van de Raad van Bestuur of de Medewerker die door de Raad van Bestuur is aangesteld om relevante functies uit te voeren (hierna in dit hoofdstuk - Interne Controlefunctionaris). De interne controlefunctionaris moet beschikken over de vereiste competentie, hulpmiddelen en toegang tot de relevante informatie in alle structurele eenheden van het bedrijf.

De interne controlefunctionaris voert ten minste op de volgende gebieden interne controletaken uit:

- de naleving door het bedrijf van het vastgestelde risicobeoordelingsbeleid en de risicobereidheid;
- Implementatie van CDD-maatregelen;
- uitvoering van sancties;
- de verplichting van het Bedrijf om de transactie of zakelijke relatie te weigeren en de beëindiging ervan;
- de meldingsplicht van het Bedrijf aan het FCIS;
- de opleidingsverplichting van het bedrijf met betrekking tot de AML/CFT-vereisten;
- de verplichting van het Bedrijf voor het verzamelen en bewaren van gegevens.

De exacte maatregelen voor het uitvoeren van interne controles worden bepaald door de interne controlefunctionaris en moeten overeenkomen met de grootte van het bedrijf en de aard, reikwijdte en mate van complexiteit van de activiteiten en verleende diensten.

De bureaus voor interne controle moeten ten minste de hierboven vermelde onderzoeksgebieden in overweging nemen.

De interne controlemaatregelen worden uitgevoerd op het door de interne controlefunctionaris vastgestelde tijdstip en met de door hem of haar vastgestelde frequentie, ten minste eenmaal per maand, indien de aard van de maatregel niet uitdrukkelijk anders bepaalt.

De resultaten van de uitvoering van interne controlemaatregelen (hierna in dit hoofdstuk: de internecontrolegegevens) worden gescheiden van andere gegevens opgeslagen en binnen vijf jaar bewaard. Alleen de leden van de raad van bestuur en de interne controlefunctionaris hebben toegang tot de interne controlegegevens.

Controlegegevens. De interne controlefunctionaris mag alleen met voorafgaande toestemming van de raad van bestuur andere werknemers of derden (bijv. adviseurs, auditors, enz.) toegang geven tot de interne controlegegevens. De personen die toegang hebben tot de interne controlegegevens mogen deze gegevens aan niemand bekendmaken zonder voorafgaande toestemming van de raad van bestuur.

De interne controlegegevens worden in chronologische volgorde opgeslagen in een formaat dat het mogelijk maakt deze te analyseren en begrijpelijk te koppelen aan andere relevante gegevens.

De interne controlefunctionaris zal het interne controleverslag ten minste elk kwartaal aan de raad van bestuur en ten minste elk jaar aan de algemene vergadering van aandeelhouders van het bedrijf voorleggen. Het interne controleverslag bevat ten minste het volgende:

- periode van het uitvoeren van de interne controle;
- naam en functie van de persoon die de interne controle uitvoert;
- beschrijving van de interne controlemaatregelen die zijn uitgevoerd;
- resultaten van de interne controle;
- algemene conclusies uit de uitgeoefende interne controle;
- vastgestelde tekortkomingen, die werden weggewerkt in de periode waarin de interne controle werd uitgevoerd;
- vastgestelde tekortkomingen, die aan het einde van de periode waarin de interne controle werd uitgevoerd, nog niet waren verholpen;
- maatregelen die uitgevoerd moeten worden om de vastgestelde tekortkomingen te verhelpen.

De raad van bestuur beoordeelt het interne controleverslag en neemt hierover een besluit. De interne controlefunctionaris wordt op de hoogte gesteld van de essentie van een dergelijk besluit in een formaat dat schriftelijk kan worden weergegeven. Om deze reden is de raad van bestuur verplicht om:

- de resultaten van de uitgevoerde interne controle analyseren;
- acties uit te voeren om tekortkomingen te verhelpen.

Het bedrijf moet de interne controleprocedure ten minste jaarlijks en in de volgende gevallen herzien en, indien nodig, bijwerken:

- na de publicatie door de Europese Commissie van de resultaten van een EU-brede risicobeoordeling van het witwassen van geld en de financiering van terrorisme (beschikbaar op de website van de Europese Commissie <http://ec.europa.eu>);
- na de publicatie van de resultaten van de Nationale Risicobeoordeling inzake Witwassen en Terrorismefinanciering (gepubliceerd in de sectie "Nationale Risicobeoordeling inzake Witwassen en Terrorismefinanciering" van de sectie "Preventie van Witwassen" van de website www.fnrt.it);
- na ontvangst van een instructie van FCIS om de toepasselijke interne controleprocedures te versterken;

- in geval van belangrijke gebeurtenissen of wijzigingen in het beheer en de activiteiten van de exploitant van het depot voor virtuele-valutageld en de exploitant van de virtuele-valutawissel.

Risicobeoordeling en risicobereidheid

Het doel van de implementatie van interne controlemaatregelen voor de naleving door het bedrijf van het vastgestelde risicobeoordelingsbeleid (inclusief de vastgestelde risicobereidheid) is het onderzoeken van de volgende omstandigheden:

- Bedrijf stelt een risicogebaseerde aanpak op en gebruikt deze bij het leveren van diensten aan Klanten (bijv. CDD-maatregelen geïmplementeerd in overeenstemming met risiconiveau);
- De onderneming heeft factoren vastgesteld die van invloed zijn op het ontstaan van ML/TF-risico's en deze factoren zijn relevant;
- Bedrijf heeft de ML/TF bepaald en beoordeeld van alle diensten die Bedrijf levert;
- Het bedrijf stelt het risicoprofiel van de Klant samen voordat het transacties uitvoert of een zakelijke relatie aangaat;
- Het bedrijf werkt het risicoprofiel van de Klant regelmatig bij;
- Bedrijf volgt vastgestelde risicobereidheid;
- Bedrijf houdt gegevens bij van alle incidenten in overeenstemming met het vastgestelde risicobeoordelingsbeleid;
- Het risicobeoordelingsbeleid werd het afgelopen jaar herzien en er is geen informatie dat MLRO eerder herziening nodig had.

Implementatie van klantenonderzoeksmatregelen

Het doel van de implementatie van interne controlemaatregelen voor de naleving van CDD-maatregelen door het bedrijf is een onderzoek van de volgende omstandigheden:

- het Bedrijf past CDD-maatregelen voorgeschreven door de Richtlijnen toe op alle relevante Klanten;
- het bedrijf verzamelt de juiste documenten en informatie bij het toepassen van CDD-maatregelen;
- het bedrijf de verzamelde gegevens en documenten bij het toepassen van CDD-maatregelen naar behoren verifieert;
- het bedrijf past het relevante niveau van CDD-maatregelen toe (bijv. EDD-maatregelen, enz.);
- het Bedrijf past de juiste EDD-maatregelen toe op specifieke Klanten (bijv. PEP, land met hoog risico, etc.);
- het Bedrijf voert de identificatie van Klanten uit in overeenstemming met de vastgestelde procedure;
- het Bedrijf de vertegenwoordiger(s) van de Klant naar behoren identificeert;
- het bedrijf de uiteindelijke begunstigen van de klanten naar behoren identificeert;
- het Bedrijf de PEP-status van Klanten correct identificeert;

- het bedrijf het doel en de aard van de zakelijke relatie of transactie goed identificeert;
- het Bedrijf zakelijke relaties met Klanten goed bewaakt.

Bij het toepassen van de EDD-maatregelen met betrekking tot de natuurlijke personen/rechtspersonen die woonachtig/gevestigd zijn in derde landen met een hoog risico, bepaald door de Europese Commissie, moet het Company:

- aanvullende informatie over de Klant en BO te verkrijgen;
- aanvullende informatie te verkrijgen over de beoogde aard van de Zakelijke Relatie;
- informatie inwinnen over de geldbron en het vermogen van de Klant en BO;
- informatie te verkrijgen over de redenen voor de voorgenomen of voltooide transacties;
- de goedkeuring verkrijgen van de Senior Manager om Zakelijke Relaties aan te gaan met deze Klanten of toestemming geven om Zakelijke Relaties met deze Klanten voort te zetten
- EDD uit te voeren door het aantal en de timing van de controles te verhogen en de soorten transacties te selecteren die nader onderzoek vereisen;
- ervoor zorgen dat de eerste betaling door een Klant wordt verricht vanaf een rekening bij een kredietinstelling wanneer die kredietinstelling is gevestigd in een EU-lidstaat of in een derde land dat eisen stelt die gelijkwaardig zijn aan die van de Wet en onder toezicht staat van de bevoegde autoriteiten.

Momenteel worden de derde landen met een hoog risico die door de Europese Commissie zijn vastgesteld, opgesomd in de Gedelegeerde Verordening nr. 2016/1675 van de Commissie van 14 juli 2016 tot aanvulling van Richtlijn (EU) 2015/849 van het Europees Parlement en de Raad door derde landen met een hoog risico en strategische tekortkomingen te identificeren, en gewijzigd bij de volgende verordeningen:

Gedelegeerde Verordening nr. 2018/105 van de Commissie van 27 oktober 2017 tot wijziging van Gedelegeerde Verordening (EU) 2016/1675, wat betreft de toevoeging van Ethiopië aan de lijst van derde landen met een hoog risico in de tabel in punt I van de bijlage;

Gedelegeerde Verordening nr. 2018/212 van de Commissie van 13 december 2017 tot wijziging van Gedelegeerde Verordening (EU) 2016/1675 ter aanvulling van Richtlijn (EU) 2015/849 van het Europees Parlement en de Raad, wat betreft de toevoeging van Sri Lanka, Trinidad en Tobago en Tunesië aan de tabel in punt I van de bijlage;

Gedelegeerde Verordening nr. 2018/1467 van de Commissie van 27 juli 2018 tot wijziging van Gedelegeerde Verordening (EU) 2016/1675 ter aanvulling van Richtlijn (EU) 2015/849 van het Europees Parlement en de Raad, wat betreft de toevoeging van Pakistan aan de tabel in punt I van de bijlage.

Op basis van de resultaten van de Nationale Risicobeoordeling Witwassen van Geld en Terrorismefinanciering, in het geval dat er een hoog niveau van ML/TF-risico's in de Republiek Litouwen wordt geïdentificeerd met betrekking tot de derde landen met een hoog risico bepaald door de Europese Commissie, moet het Bedrijf, wanneer het internationale correspondentrelaties aangaat of uitvoert met financiële instellingen die in deze landen gevestigd zijn, een of meerdere aanvullende maatregelen nemen om het risico op ML/TF effectief te verminderen:

- aanvullende maatregelen toepassen voor verscherpt toezicht op zakenrelaties om het risico op witwassen en financiering van terrorisme te verminderen;
- de melding van verdachte geldtransacties en -transacties strenger maken;
- de Zakelijke Relaties of transacties beperken met natuurlijke personen of rechtspersonen die gevestigd zijn in derde landen met een hoog risico die door de Europese Commissie zijn geïdentificeerd.

Als deze aanvullende maatregelen niet voldoende zijn om dit risico te verminderen, moet het Bedrijf weigeren om een internationale correspondentrelatie met dergelijke financiële instellingen aan te gaan, deze stopzetten of beëindigen.

Op dit moment staan de derde landen met een hoog risico op de FATF-lijsten van landen die ernstige tekortkomingen hebben op het gebied van de preventie van ML/TF en de bestrijding van deze misdrijven: <http://www.fatf-gafi.org/countries/#high-risk>. Aangezien de lijst echter verandert, moet het bedrijf controleren of de lijst niet is gewijzigd en indien nodig passende maatregelen nemen.

Bij het toepassen van de EDD-maatregelen met betrekking tot natuurlijke personen/rechtspersonen die woonachtig/gevestigd zijn in derde landen met een hoog risico die zijn opgenomen in de FATF-lijsten van staten die ernstige tekortkomingen vertonen op het gebied van de preventie van het witwassen van geld/de financiering van terrorisme en de bestrijding van deze misdrijven, moet het bedrijf:

- goedkeuring ontvangen van de Senior Manager om een Zakelijke Relatie aan te gaan met die Klanten of om de Zakelijke Relatie met die Klanten voort te zetten;
- passende maatregelen nemen om de bron van rijkdom en de bron van fondsen met betrekking tot de Zakelijke relatie of transactie vast te stellen;
- een verbeterde, voortdurende controle uitvoeren van de Zakelijke Relatie met dergelijke Klanten.

Bij het bepalen welke Klanten hoge ML/TF-risico's met zich meebrengen, moet het Bedrijf een risicobeoordeling uitvoeren op de Zakelijke Relaties. Rekening houdend met de uitkomsten van ten minste de risicobeoordeling van het Bedrijf, de nationale risicobeoordeling en de supranationale risicobeoordeling, moet het Bedrijf bijzondere zorgvuldigheid betrachten bij het beoordelen van de ML/TF-risico's die mogelijk worden veroorzaakt door de volgende personen en entiteiten:

- handelaren in goederen die in het kader van hun bedrijfsactiviteiten gewoonlijk aanzienlijke bedragen in contanten betalen of ontvangen;
- entiteiten die actief zijn in de financiële subsectoren of producten die met contant geld werken (bijv. wisselkantoren, geldovermakingen, bepaalde elektronisch-geldproducten);
- bepaalde FinTech-bedrijven (d.w.z. op technologie gebaseerde en door technologie ondersteunde financiële dienstverleners), vooral met een groot aantal zakelijke relaties die niet persoonlijk zijn;
- exploitanten van uitwisselingsplatforms voor virtuele valuta en/of aanbieders van portemonnees;

- Andere Verplichte Entiteiten, met name aanbieders van gambling-diensten en/of loterijen en kansspelautomaten;
- organisaties zonder winstoogmerk;
- anderen.

Daarnaast moet het bedrijf bij het beoordelen van de mogelijke risico's op ML/TF van de klanten in het bijzonder rekening houden met:

- de Klanten waarvoor eerder een STR werd ingediend;
- de Klanten die in het verleden op internationale of nationale financiële sanctielijsten en andere lijsten stonden;
- de Klanten die het onderwerp zijn van een verzoek of informatie ontvangen van de FIU, andere autoriteiten voor gerechtelijk vooronderzoek, het Openbaar Ministerie of een rechtbank met betrekking tot informatie over een klant of zijn monetaire transacties of transacties die verband kunnen houden met ML/TF of andere criminele activiteiten.

Bij het bepalen of er sprake is van een hoger risico op ML/TF moet de Vennootschap ten minste de volgende factoren beoordelen:

- kenmerken van de Klant:
- de Zakelijke Relatie van de Klant wordt uitgevoerd onder ongebruikelijke omstandigheden die geen duidelijk economisch of zichtbaar rechtmatig doel hebben;
- de woonplaats van de Klant in een derde land ligt;
- de juridische entiteiten en lichamen zonder rechtspersoonlijkheid houden zich bezig met de activiteiten van individuele vastgoedbeheermaatschappijen;
- het bedrijf formele aandeelhouders heeft die voor een andere persoon optreden, of aandelen aan toonder heeft;
- contant geld overheerst in het bedrijf;
- de vermogensstructuur van de rechtspersoon kennelijk ongebruikelijk of buitengewoon complex is gezien de aard van de activiteiten van de rechtspersoon,
- kenmerken van het product, de dienst, de transactie of het servicekanaal:
- particulier bankieren;
- product of transactie kan gunstige voorwaarden voor anonimiteit creëren;
- Zakelijke relaties of incidentele transacties worden afgesloten of uitgevoerd zonder fysieke aanwezigheid;

- betalingen worden ontvangen van onbekende of niet-gerelateerde derden;
- product of bedrijfspraktijk, inclusief het dienstverleningsmechanisme, nieuw zijn, evenals het gebruik van nieuwe of zich ontwikkelende technologieën die betrokken zijn bij het werk met zowel nieuwe als oude producten,
- kenmerken van het grondgebied:
 - volgens de gegevens van rapporten of gelijkaardige documenten van de FAG of een andere gelijkaardige regionale organisatie, het systeem voor de bestrijding van witwassen en financiering van terrorisme in aanzienlijke mate niet voldoet aan de internationale vereisten;
 - volgens de gegevens van gouvernementele en wereldwijd erkende niet-gouvernementele organisaties die het corruptieniveau controleren en beoordelen, is een hoog niveau van corruptie of andere criminele activiteiten in de staat is vastgesteld;
 - de staat is onderworpen aan sancties, embargo's of soortgelijke maatregelen die bijvoorbeeld door de EU of de Verenigde Naties zijn opgelegd;
 - de staat terroristische activiteiten financiert of ondersteunt, of terroristische organisaties die op de lijsten van internationale organisaties staan op het grondgebied van de staat actief zijn.

Implementatie van sancties

Het doel van de implementatie van interne controlemaatregelen voor de naleving door het bedrijf van de implementatie van sancties is een onderzoek van de volgende omstandigheden:

- de Vennootschap past de procedure toe voor de identificatie van een onderwerp van Sancties of een transactie die Sancties schendt;
- het Bedrijf voert acties uit als het een onderwerp van Sancties of een transactie die Sancties schendt, identificeert.

Verplichting tot weigering van transactie of zakelijke relatie en de beëindiging ervan

Het doel van de implementatie van interne controlemaatregelen voor de naleving door het bedrijf van de verplichting om de transactie of zakelijke relatie te weigeren en hun beëindiging is een onderzoek van de volgende omstandigheden:

- het Bedrijf weigert een transactie of zakelijke relatie als dit verplicht is volgens de Richtlijnen;
- het Bedrijf weigert of beëindigt een transactie of zakelijke relatie als dit verplicht is volgens de Richtlijnen.

Rapportageverplichting

Het doel van de implementatie van interne controlemaatregelen voor de naleving van de verslagleggingsverplichting door het bedrijf is een onderzoek van de volgende omstandigheden:

- het Bedrijf stuurt rapporten en informatie naar FCIS, als dit vereist wordt door de Richtlijnen (incl. relevante FCIS-richtlijnen);
- de rapporten die naar FCIS worden gestuurd, worden ingevuld in overeenstemming met de richtlijnen van FCIS.

Trainingsverplichting

Het doel van de implementatie van interne controlemaatregelen voor de naleving door het bedrijf van de trainingsverplichting op AML/CTF-gebied is een onderzoek van de volgende omstandigheden:

- alle werknemers (inclusief MLRO en leden van de raad van bestuur) relevante training hebben gehad;
- elke werknemer (incl. MLRO en leden van de raad van bestuur) de afgelopen 360 dagen training heeft gevolgd.

Verplichting om gegevens te verzamelen en te bewaren

Het doel van de implementatie van interne controlemaatregelen voor de naleving door het bedrijf van de verplichting om gegevens te verzamelen en te bewaren, is een onderzoek van de volgende omstandigheden:

- alle gegevens die moeten worden opgeslagen in overeenstemming met de Richtlijnen (hierna in dit hoofdstuk - de Opgeslagen Gegevens) correct zijn opgeslagen in chronologische volgorde met een indeling die het mogelijk maakt om deze te analyseren en de Opgeslagen Gegevens begrijpelijk te verbinden met andere relevante gegevens;
- alleen Werknemers (incl. MLRO en leden van de Raad van Bestuur) of bevoegde derden hebben toegang tot de Opgeslagen Gegevens;
- alle relevante logboeken worden bijgehouden in overeenstemming met de Richtlijnen;
- de Opgeslagen gegevens in elektronisch formaat een back-up heeft;
- de Opgeslagen Gegevens in andere formaten (bijv. op papier) een back-up in elektronisch formaat hebben;
- worden de Opgeslagen Gegevens onherroepelijk verwijderd in overeenstemming met de Richtlijnen.

BIJLAGEN

Bijlage titel	Beschrijving van het document
Beleid voor risicobeoordeling	Stelt principes vast voor het risicobeheer van het bedrijf (incl. risicobeoordeling en risicofactoren) met betrekking tot het witwassen van geld en de bescherming van de financiële belangen van het bedrijf. Risico's van terrorismefinanciering.
Profielen van klanten	Tabel voor de risicobeoordeling van Klanten en het documenteren van deze beoordeling. Inclusief risicofactoren van elke risicocategorie.
Inwerkprocedure voor klanten	Stelt de instructies voor onboarding van de klant vast die worden gebruikt bij de implementatie van CDD-maatregelen
Vragenlijsten	Er wordt een bepaalde hoeveelheid informatie gevraagd bij het uitvoeren van CDD-maatregelen (incl. toepassing van EDD-maatregelen, SoW/SoF vragen, enz.)
Lijst van bronnen	Bevat een niet-uitputtende lijst van middelen die gebruikt kunnen worden voor de implementatie van CDD-maatregelen.
Lijst van criteria voor het witwassen van geld en de identificatie van verdachte geldtransacties of -transacties	Instructies en voorbeelden van transacties en andere omstandigheden die vanuit het oogpunt van ML/TF als verdacht moeten worden beschouwd.
De lijst van Werknemers en hun verantwoordelijkheden	De lijst van Werknemers met hun aansprakelijkheden binnen de gespecificeerde Richtlijnen
Logboeken	De tabel wordt gebruikt voor het bijhouden van de logboeken.
MLRO rapportageformulier	Het rapportageformulier, dat de MLRO elk kwartaal aan de raad van bestuur zal verstrekken
Richtlijnen voor het invullen van de formulieren voor het indienen van informatie bij FCIS	FCIS-richtlijnen voor het invullen van relevante formulieren en formulieren zelf.

Opschorting van verdachte monetaire transacties of verrichtingen en indiening van informatie over verdachte monetaire transacties of verrichtingen bij het FCIS	De relevante FCIS-richtlijnen.
Technische vereisten voor klantidentificatie via live videotransmissie	FCIS-richtlijnen voor de relevante technische vereisten
Trainingsprotocol	Het ontwerp van het document dat ingevuld moet worden voor elke training die het Bedrijf geeft aan de Relevante Personen (inclusief het vertrouwd maken met de Richtlijnen).
Resolutie ter goedkeuring van de richtlijnen	Het ontwerpbesluit van het senior management van het bedrijf ter goedkeuring van deze richtlijnen.

VERSIEBEHEER TABEL

Versie	Goedkeuringsdatum	Veranderingen Beschrijving
1.0	dd.mm.jjjj	Eerste uitgave
1.1	28.03.2023	Bijgewerkte versie
1.2	11.07.2023	Bijgewerkte versie
2.0	07.08.2023	Tweede uitgave
2.1	06.12.2023	Bijgewerkte versie
2.2	18.03.2024	Bijgewerkte versie

Mariana Achim
 18.03.2024