uexo \ Myrtle Ltd \ FSC

Handbuch zur AML-CFT-Einhaltung

v1.5

Inhaltsübersicht

1. Einführung

Die Marke uexo ist in verschiedenen Rechtsordnungen zugelassen und reguliert, wobei die mauritische Einheit im Besitz von Myrtle Limited ist und von dieser betrieben wird. Myrtle Limited (im Folgenden als "uexo" oder "Gesellschaft" bezeichnet) hat seine Adresse in Suite 803, 8th Floor, Hennessy Tower, Pope Hennessy Street, 11328, Port Louis, Mauritius. Das Unternehmen unterliegt der Aufsicht der Mauritius Financial Services Commission (FSC) als Investment Dealer (Broker) mit der Lizenznummer GB21026300.

Im Jahr 2002 wurde in Mauritius das Gesetz zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung (Financial Intelligence and Anti Money Laundering Act - FIAMLA) erlassen. Der mauritische Rahmen zur Bekämpfung der Geldwäsche und der Terrorismusfinanzierung wurde durch das FIAMLA und später durch die Financial Intelligence and Anti Money Laundering Regulations 2003 festgelegt. Die Verordnungen von 2003 wurden 2018 geändert und sind nun als Financial Intelligence and Anti Money Laundering Regulations 2018 bekannt.

Die Gesellschaft fällt unter die Definition einer meldepflichtigen Person im Sinne von Abschnitt 2 des FIAMLA 2002. Die Gesellschaft muss sicherstellen, dass die einschlägigen Anforderungen des FIAMLA 2002, der FIAML-Verordnungen 2018, des United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Act 2019 und anderer Regeln, Vorschriften, Rundschreiben, Kodizes oder Richtlinien, die von Zeit zu Zeit von der FSC herausgegeben werden, kontinuierlich eingehalten werden.

Das Unternehmen verpflichtet sich, sicherzustellen, dass seine Geschäftstätigkeiten in Übereinstimmung mit den geltenden rechtlichen und regulatorischen Standards durchgeführt werden. Das Compliance-Handbuch zur Bekämpfung der Geldwäsche und der Finanzierung des Terrorismus (im Folgenden "AML-CFT-Handbuch" oder "Compliance-Handbuch" oder "Handbuch") soll die Einhaltung der Anforderungen des FIAMLA, der Financial Intelligence and Anti Money Laundering Regulations 2018, des UN Sanctions Act 2019 und aller anderen geltenden Gesetze und Nebengesetze sicherstellen. Ziel des AML-CFT-Handbuchs ist es, das Unternehmen und seine Mitarbeiter in die Lage zu versetzen, die von seiner Aufsichtsbehörde, der FSC, vorgeschriebenen Maßnahmen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung (AML-CFT) anzuwenden und somit Verstößen vorzubeugen.

Das vorliegende AML-CFT-Compliance-Handbuch gibt den aktuellen Stand der Gesetzgebung wieder. Es ist daher mindestens einmal jährlich zu überprüfen, um seine Angemessenheit und Wirksamkeit zu gewährleisten und um etwaige Änderungen der geltenden Gesetze und Vorschriften zu berücksichtigen.

Dieses AML-CFT-Compliance-Handbuch gilt für das Unternehmen und alle seine gegenwärtigen und zukünftigen Tochtergesellschaften. Von den Mitarbeitern, einschließlich Vertretern/Beauftragten, die an der Erbringung der vorgeschriebenen Dienstleistungen beteiligt sind, wird erwartet, dass sie den Inhalt dieser Richtlinie kennen und verstehen und sich an die darin enthaltenen Standards halten. Jeder Mitarbeiter, der gegen diese Richtlinie verstößt, muss mit Disziplinarmaßnahmen rechnen, die der Vorstand für angemessen hält.

Alle betroffenen Mitarbeiter des Unternehmens müssen das in Anhang 9 enthaltene Bestätigungsformular unterzeichnen, um zu zeigen, dass das Handbuch an sie verteilt wurde und dass sie es gelesen und verstanden haben und sich verpflichten, die Anforderungen des Handbuchs einzuhalten.

2. Definitionen und Auslegungen

1. **AML-CFT**
   Bedeutet Anti-Geldwäsche und Bekämpfung der Finanzierung des Terrorismus.

2. **Kunde**
   bezeichnet jede natürliche oder juristische Person oder Rechtsvereinbarung, die eine Geschäftsbeziehung oder eine einmalige Transaktion mit/über das Unternehmen anstrebt.

3. **Begünstigter Eigentümer**
   bezeichnet die natürliche Person, die letztlich Eigentümer einer juristischen Person oder Rechtsvereinbarung ist oder diese kontrolliert, und/oder die Person, in deren Namen eine Transaktion durchgeführt wird. Der Begriff umfasst die natürliche Person, die die letztendliche Kontrolle über eine juristische Person oder Rechtsvereinbarung ausübt, sowie andere natürliche Personen, wie nachstehend beschrieben:
   a. die letztlich die Kontrolle über eine juristische Person innehat
   b. bei Zweifeln in Bezug auf (A) die natürliche Person, die eine Mehrheitsbeteiligung hält, oder die natürliche Person, die die Kontrolle über die juristische Person auf andere Weise ausübt
   c. in Fällen, in denen keine natürliche Person gemäß Buchstabe A oder B identifiziert werden kann, die Identität der natürlichen Person, die die Position eines leitenden Angestellten innehat.

4. **Geschäftsbeziehung**
   Bezeichnet eine vertragliche Beziehung zwischen dem Unternehmen und einem Kunden über die Bereitstellung von Produkten oder Dienstleistungen durch das Unternehmen für den Kunden auf häufiger, gewohnheitsmäßiger, regelmäßiger oder einmaliger Basis.

5. **CDD**
   Bedeutet Customer Due Diligence.

6. **Benannte Partei**
   Means any individual, group, undertaking or entity declared as a designated party by the Secretary for Home Affairs following direction by the National Sanctions Committee under section 9 or 10 of the UN Sanctions Act.

7. **EDD**
   Bedeutet verstärkte Sorgfaltspflicht.

8. **FIAMLA**
   Der Financial Intelligence and Anti-Money Laundering Act 2002.

9. **FIAMLR**
   Bedeutet: The Financial Intelligence and Anti-Money Laundering Regulations 2018.

10. **FIU**
    Die Financial Intelligence Unit wurde gemäß Abschnitt 9 des FIAMLA eingerichtet.

11. **FSC-Handbuch**
    Bezeichnet das vom FSC herausgegebene AML/CFT-Handbuch

12. **Juristische Person**
    Bedeutet
    a. jede andere juristische Person als eine natürliche Person, die eine dauerhafte Geschäftsbeziehung mit dem Unternehmen eingehen oder anderweitig Eigentum besitzen kann;
    b. und umfasst ein Unternehmen, eine Stiftung, einen Verein, eine Kommanditgesellschaft oder eine andere von der FIU oder einer zuständigen Aufsichtsbehörde vorgeschriebene Einrichtung.

13. **Rechtliche Regelung**
    Bezeichnet einen Trust oder eine ähnliche Einrichtung.

14. **Gelistete Partei**
    Bezeichnet eine Person, eine Gruppe, ein Unternehmen oder eine Einrichtung, die vom Sicherheitsrat der Vereinten Nationen oder unter dessen Aufsicht in der konsolidierten Liste des Sicherheitsrats der Vereinten Nationen - auch bekannt als UN-Sanktionsliste - aufgeführt ist.

15. **MLRO**
    Bedeutet Geldwäsche-Meldebeauftragter.

16. **ML/TF**
    Bedeutet Geldwäsche, Terrorismusfinanzierung und Proliferationsfinanzierung.

17. **Einzelne**
    Bezeichnet ein lebendes menschliches Wesen, das rechtlich in der Lage ist, einen verbindlichen Vertrag mit dem Unternehmen (oder seinen Tochtergesellschaften) abzuschließen.

18. **NRA**
    Bezeichnet die nationale Bewertung des Risikos der Geldwäsche und der Terrorismusfinanzierung in Mauritius, die vom Ministerium für Finanzdienstleistungen und gute Regierungsführung im August 2019 veröffentlicht wurde.

19. **PEP**
    Bedeutet eine politisch exponierte Person. Politisch exponierte Personen sind Personen, die mit herausragenden öffentlichen Funktionen/Positionen betraut sind oder waren (z. B. Staatsoberhäupter oder Regierungschefs, hochrangige Politiker, hochrangige Regierungs-, Justiz- und Militärbeamte, leitende Angestellte staatlicher Unternehmen und wichtige Parteifunktionäre), sowie deren Verwandte und Mitarbeiter. Dies schließt ein:
    a. Personen, die die Definition eines PEP in Mauritius erfüllen (inländische PEP),
    b. Personen, die die Definition eines PEP in einem anderen Land erfüllen (ausländische PEP) und

c. Personen, die von einer internationalen Organisation mit einer herausgehobenen Funktion/Position betraut wurden, einschließlich Mitgliedern des oberen Managements oder anderen Funktionen, die Direktoren, stellvertretenden Direktoren und Mitgliedern des Verwaltungsrats entsprechen (PEP einer internationalen Organisation).
d. Dazu gehören auch enge Mitarbeiter und Familienangehörige von PEPs, wie unten definiert:
    i. Familienmitglieder
        1. eine Person, die mit einer PEP entweder direkt durch Blutsverwandtschaft oder durch Heirat oder ähnliche Formen der Lebenspartnerschaft verwandt ist; und
        2. schließt jede andere Person ein, die von einer Aufsichtsbehörde oder Regulierungsstelle nach Rücksprache mit dem Nationalen Ausschuss festgelegt werden kann.
    ii. Enge Verbündete
        1. eine Person, die mit einer PEP entweder gesellschaftlich oder beruflich eng verbunden ist; und
        2. schließt jede andere Person ein, die von einer Aufsichtsbehörde oder Regulierungsstelle nach Rücksprache mit dem Nationalen Ausschuss festgelegt werden kann.

20. **Schulleiter**

Bezeichnet jede natürliche oder juristische Person, die entweder direkt oder indirekt:

a. in der Lage ist, die Geschäftstätigkeit oder die Finanzgeschäfte einer juristischen Person/juristischen Vereinbarung zu kontrollieren oder einen erheblichen Einfluss darauf auszuüben,
b. die Befugnis hat, ein Mitglied des Leitungsorgans der juristischen Person/juristischen Vereinbarung zu ernennen oder abzuberufen,
c. eine Person zum Mitglied des Leitungsorgans der juristischen Person/Rechtsvereinbarung ernennen oder abberufen kann,
d. wirtschaftlicher Eigentümer der juristischen Person/Rechtsvereinbarung ist,
e. eine juristische Person/Rechtsvereinbarung mit ihrem Anfangsvermögen ausgestattet hat,
f. einer juristischen Person/Rechtsvereinbarung Vermögen übertragen oder eine letztwillige Verfügung getroffen hat.

Handelt es sich bei dem Kunden um ein Unternehmen, so sind unter Auftraggebern die Geschäftsführer, Anteilseigner, wirtschaftliche(n) Eigentümer und Bevollmächtigte zu verstehen.

Handelt es sich bei dem Kunden um eine Personengesellschaft, sind unter Auftraggebern der/die Komplementär(e), der/die Kommanditist(en), der/die wirtschaftlich Berechtigte(n) und die Bevollmächtigten zu verstehen.

Handelt es sich bei dem Kunden um einen Treuhandfonds, sind Auftraggeber der Treugeber, der Treuhänder, der/die Begünstigte(n), der Vollstrecker und/oder Protektor (falls vorhanden) und die Bevollmächtigten des Treuhänders.

Handelt es sich bei dem Kunden um eine Stiftung, so bezeichnen die Auftraggeber den Stifter, die Mitglieder des Rates, den/die Begünstigten und die Bevollmächtigten.

Handelt es sich bei dem Kunden um eine "société", sind die Auftraggeber: der "gérant", die "associés", der "bénéficiaire effectif" und die Bevollmächtigten

21. **Verordnung**
    Bedeutet eine Regulierung gemäß den Financial Intelligence and Anti-Money Laundering Regulations 2018.

22. **STR**
    Bedeutet Bericht über verdächtige Transaktionen.

23. **UN-Sanktionsgesetz**
    Bedeutet: Gesetz über die Sanktionen der Vereinten Nationen (Finanzverbote, Waffenembargo und Reiseverbot) 2019.

24. **UN**
    Bedeutet, dass die Organisation der Vereinten Nationen im Jahr 1945 gegründet wurde.

25. **UN-Sanktionsliste**
    bezeichnet die konsolidierte Liste des Sicherheitsrates der Vereinten Nationen.

In dieser Richtlinie schließt die Verwendung des männlichen, weiblichen oder sächlichen Geschlechts auch die anderen Geschlechter ein, und die Verwendung des Singulars schließt den Plural ein und umgekehrt.

3. Geldwäsche, Terrorismusfinanzierung und Finanzierung der Proliferation

Geldwäsche kann als Prozess beschrieben werden, bei dem die Herkunft von Erträgen aus Straftaten verschleiert wird, indem sie beispielsweise durch eine komplexe Abfolge von Banküberweisungen oder Handelstransaktionen geleitet werden, mit dem letztendlichen Ziel, die illegal erwirtschafteten Erlöse als legal erscheinen zu lassen. Geldwäsche wird oft fälschlicherweise als eine Aktivität angesehen, die nur mit organisierter Kriminalität und Drogenhandel in Verbindung gebracht wird. Geldwäsche liegt jedoch immer dann vor, wenn eine (natürliche oder juristische) Person mit direkten oder indirekten Erträgen aus einer Handlung oder Unterlassung handelt, die gegen das Gesetz verstößt, sei es Erpressung, Diebstahl, Betrug, Steuerhinterziehung, Entführung, Bestechung, Verletzung von Urheberrechten, kreative Buchführung usw. Auch wenn die Straftat als "Geldwäsche" bezeichnet wird, handelt es sich um jede Form von materiellem oder immateriellem Eigentum und nicht nur um Bargeld, das direkt oder indirekt einen Gewinn aus einem Verbrechen darstellt.

Geldwäsche wird in der Regel als ein dreistufiger Prozess beschrieben:

1. **Platzierung**
   In der ersten Phase werden die illegalen Gelder in das legale Finanzsystem eingeschleust. Dies geschieht beispielsweise durch die Einzahlung kleiner Beträge auf Bankkonten oder durch falsche Rechnungsstellung. Diese Phase dient zwei Zwecken: (i) Sie entlastet den Kriminellen von der Aufbewahrung und Bewachung großer Bargeldbeträge, und (ii) sie führt die illegalen Gelder in das legale Finanzsystem ein.

2. **Schichtung**
   Der Hauptzweck der Schichtungsphase besteht darin, die illegalen Gelder von der ursprünglichen Straftat zu trennen, indem komplexe Strukturen und Transaktionen (Schichten) verwendet werden, um den Prüfpfad zu verschleiern. Die Geldwäscher können beispielsweise damit beginnen, die Gelder elektronisch von einem Land in ein anderes zu verschieben, das Bargeld in Geldinstrumente umzuwandeln oder Rückzahlungsvereinbarungen zu treffen.

3. **Integration**
   Die letzte Phase des Geldwäscheschemas. Die Gelder wurden vollständig in die legale Wirtschaft integriert, so dass der Kriminelle die Gelder durch eine scheinbar legale Transaktion zurückerhalten kann. Zum Beispiel durch den Kauf von Immobilien oder durch Investitionen auf den Wertpapiermärkten.

Finanzierung von Terrorismus

Unter Terrorismusfinanzierung hingegen versteht man die Beschaffung oder Bereitstellung von Finanzmitteln oder nicht-finanzieller Unterstützung für terroristische Organisationen. Diese Organisationen benötigen Finanzmittel nicht nur zur Finanzierung spezifischer terroristischer Aktionen, sondern auch zur Deckung der organisatorischen Kosten für den Aufbau und die Aufrechterhaltung einer terroristischen Vereinigung und zur Schaffung eines günstigen Umfelds, das sie zur Aufrechterhaltung ihrer Aktivitäten benötigen. Terroristische Organisationen können sich aus legalen Quellen finanzieren, z. B. durch den Missbrauch von karitativen Einrichtungen oder legalen Unternehmen oder durch die Selbstfinanzierung der Terroristen selbst. Terroristen finanzieren sich auch aus einer Vielzahl von kriminellen Aktivitäten.

Die wichtigsten Unterschiede zwischen Geldwäsche und Terrorismusfinanzierung sind:

- ★ Im Falle der Geldwäsche stammen die Gelder/Vermögenswerte immer aus rechtswidrigen Tätigkeiten, während im Falle der Terrorismusfinanzierung die Gelder/Vermögenswerte sowohl aus legalen als auch aus kriminellen Quellen stammen können; und

- ★ Das eigentliche Ziel der Geldwäscher besteht darin, die Herkunft der illegalen Gelder/Vermögenswerte zu verschleiern, während Personen, die an der Finanzierung des Terrorismus beteiligt sind, verschleiern wollen, dass sie Terrorakte oder terroristische Organisationen finanzieren.

Es gibt auch Gemeinsamkeiten zwischen Geldwäsche und Terrorismusfinanzierung; dazu gehören:

- ★ Kriminelle Aktivitäten - Terroristen gehen auch anderen Straftaten nach, wie z. B. dem Drogen- oder Menschenhandel, um ihre Aktivitäten zu finanzieren;

- ★ Sowohl Geldwäscher als auch Geldgeber des Terrorismus nutzen Finanzinstitute und Finanzdienstleister.

Finanzierung der Proliferation

Proliferation bezeichnet die Entwicklung und den Einsatz nuklearer, chemischer oder biologischer Waffen - auch bekannt als Massenvernichtungswaffen - und ihrer Trägersysteme unter Verstoß gegen internationale Abkommen und Ausfuhrkontrollregelungen.

Proliferationsfinanzierung bezieht sich auf die Finanzierung der Verbreitung von Massenvernichtungswaffen, einschließlich, aber nicht beschränkt auf die Weitergabe oder den Export von Technologie, Waren, Software, Dienstleistungen oder Fachwissen, die in Programmen mit nuklearen, biologischen oder chemischen Waffen und deren Trägersystemen verwendet werden können. Personen, die an Systemen zur Finanzierung von Proliferation und Weiterverbreitung beteiligt sind, nutzen komplexe Netze von Scheinfirmen und von Geldwäschern abgeleitete Abzweigungstechniken, um Zugang zum globalen Finanzsystem zu erhalten und die immer strengeren Maßnahmen zur Bekämpfung der Proliferationsfinanzierung zu umgehen.

3.1 Straftaten gegen Geldwäsche und Terrorismusfinanzierung

Die wichtigsten Gesetze, die sich mit den Straftatbeständen Geldwäsche, Terrorismusfinanzierung und Proliferationsfinanzierung in Mauritius befassen, sind der Financial Intelligence and Anti-Money Laundering Act 2002, der Prevention of Terrorism Act 2002 bzw. der United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019.

3.1.1 Gesetz über Finanzermittlung und Geldwäschebekämpfung von 2002 (FIAMLA)

Abschnitt 3:

1. Jede Person, die
    a. sich an einer Transaktion beteiligt, bei der es um Vermögensgegenstände geht, die ganz oder teilweise direkt oder indirekt den Erlös aus einer Straftat darstellen; oder

    b. einen Vermögensgegenstand, der ganz oder teilweise direkt oder indirekt den Erlös aus einer Straftat darstellt, entgegennimmt, besitzt, verheimlicht, verschleiert, überträgt, umwandelt, veräußert, aus Mauritius verlegt oder

nach Mauritius einführt, wenn er den Verdacht oder berechtigten Grund zu der Annahme hat, dass dieser Vermögensgegenstand ganz oder teilweise direkt oder indirekt aus einer Straftat stammt oder realisiert wurde, begeht eine Straftat.

2. Eine meldende Person, die es unterlässt, die nach vernünftigem Ermessen erforderlichen Maßnahmen zu ergreifen, um sicherzustellen, dass weder sie selbst noch eine von ihr angebotene Dienstleistung von einer Person zur Begehung oder Erleichterung der Begehung einer Straftat der Geldwäsche oder der Terrorismusfinanzierung verwendet werden kann, begeht eine Straftat.

3. Die Bezugnahme auf die Verheimlichung oder Verschleierung von Vermögensgegenständen, die ganz oder teilweise direkt oder indirekt Erträge aus einer Straftat sind, schließt die Verheimlichung oder Verschleierung ihrer wahren Natur, ihrer Herkunft, ihres Standorts, ihrer Verfügung, ihrer Bewegung oder ihres Eigentums oder ihrer Rechte an ihnen ein.

Abschnitt 8:
Jede Person, die aufgrund des FIAMLA verurteilt wird, wird mit einer Geldstrafe von bis zu 2 Millionen Rupien und einer Freiheitsstrafe von bis zu 10 Jahren bestraft.

3.1.2. Gesetz zur Verhütung von Terrorismus von 2002 (POTA)

Abschnitt 6:

1. Jede Person, die in irgendeiner Weise oder Form
    a. zur Unterstützung einer terroristischen Handlung auffordert oder diese Unterstützung anbietet, oder
    b. für eine verbotene Organisation um Unterstützung wirbt oder ihr Unterstützung anbietet, begeht eine Straftat.

2. Für die Zwecke von Unterabschnitt (1) umfasst der Begriff "Unterstützung" Folgendes
    a. Anstiftung zu terroristischen Handlungen;
    b. Angebot von materieller Unterstützung, Waffen, falschen Dokumenten oder Ausweisen;
    c. die Erbringung oder Zurverfügungstellung solcher finanzieller oder sonstiger damit verbundener Dienstleistungen.

Abschnitt 15:

1. Jede Person, die eine Vereinbarung eingeht oder sich an einer solchen beteiligt, die es einer anderen Person erleichtert, terroristische Güter zurückzubehalten oder zu kontrollieren, gleich auf welche Weise, einschließlich
    a. durch Verheimlichung;
    b. durch Verbringung aus dem Hoheitsgebiet; oder
    c. durch Übergabe an eine andere Person, begeht eine Straftat.

Abschnitt 32:
Wer eine Straftat nach den §§ 6 oder 15 begeht, wird bei Verurteilung mit einer Freiheitsstrafe von mindestens 3 Jahren und höchstens 20 Jahren bedroht.

3.1.3. Das Gesetz über die Sanktionen der Vereinten Nationen (Finanzverbote, Waffenembargo und Reiseverbot) 2019 (UN-Sanktionsgesetz)

Abschnitt 23 (1):

1. Vorbehaltlich dieses Gesetzes darf niemand mit den Geldern oder den Vermögenswerten einer benannten oder aufgelisteten Partei handeln, einschließlich
    a. Alle Gelder oder sonstigen Vermögenswerte, die sich im Besitz oder unter der Kontrolle der benannten oder gelisteten Partei befinden, und nicht nur solche, die sich mit
        i. eine bestimmte terroristische Handlung, ein Komplott oder eine Drohung;
        ii. eine bestimmte Handlung, ein bestimmtes Vorhaben oder eine bestimmte Bedrohung im Zusammenhang mit der Verbreitung von Massenvernichtungswaffen;
    b. Gelder oder andere Vermögenswerte, die sich vollständig oder gemeinsam im Besitz oder unter der direkten oder indirekten Kontrolle der benannten oder aufgeführten Partei befinden;
    c. Gelder oder andere Vermögenswerte, die aus Geldern oder anderen Vermögenswerten abgeleitet oder generiert werden, die im Eigentum oder unter der direkten oder indirekten Kontrolle der benannten oder gelisteten Partei stehen, und
    d. Gelder oder andere Vermögenswerte einer Partei, die im Namen oder auf Anweisung der benannten oder aufgeführten Partei handelt.

Abschnitt 23 (5):

Wer die Bestimmungen von Absatz (1) nicht einhält, begeht eine Straftat und wird im Falle einer Verurteilung mit einer Geldstrafe von höchstens 5 Millionen Rupien oder dem doppelten Wert der Gelder oder anderer Vermögenswerte, je nachdem, welcher Betrag höher ist, und mit einer Freiheitsstrafe von mindestens drei Jahren bestraft.

3.2 Das Risiko verstehen

Durch kriminelle Aktivitäten werden riesige Mengen illegaler Gelder generiert, die in das legale Wirtschafts- und Finanzsystem integriert werden müssen, damit sie den Kriminellen zugute kommen, ohne dass die Aufmerksamkeit auf die zugrunde liegende Straftat gelenkt wird.

Nach der nationalen Risikobewertung ("NRA") wurden Anlagehändler, die über eine Zulassung als Anlagehändler (Broker) verfügen, in Bezug auf die Anfälligkeit für Geldwäsche als mittleres Risiko eingestuft. In der nationalen Risikobewertung wurde ferner festgestellt, dass die Geschäftstätigkeit von Anlagehändlern durch eine große Zahl von Kleinanlegern gekennzeichnet ist und dass die Komplexität der Produkte sowie die Art der Kunden (PEPs oder Kunden aus Hochrisikoländern) aus Sicht der Geldwäschebekämpfung und der Terrorismusbekämpfung Risiken bergen können.

Wie bereits erwähnt, beschaffen sich terroristische Organisationen Mittel sowohl aus legalen als auch aus kriminellen Quellen, um ihre Aktivitäten zu unterstützen. Daher kann die Terrorismusfinanzierung auch Geldwäsche nach sich ziehen.

4. Verpflichtung zur Einhaltung der Vorschriften

Da die Gesellschaft unter die Definition einer meldepflichtigen Person im Sinne des FIAMLA fällt, ist sie rechtlich verpflichtet, die Anforderungen sowohl des FIAMLA als auch des FIAMLR zu erfüllen.

Abschnitt 3(2) des FIAMLA besagt, dass eine meldepflichtige Person, die es versäumt, die nach vernünftigem Ermessen erforderlichen Maßnahmen zu ergreifen, um sicherzustellen, dass weder sie noch eine von ihr angebotene Dienstleistung von einer Person zur Begehung oder Erleichterung der Begehung einer Straftat der Geldwäsche oder der Terrorismusfinanzierung genutzt werden kann, eine Straftat begeht.

Das Strafmaß bei Verurteilung ist eine Geldstrafe von höchstens 10 Millionen Rupien und eine Freiheitsstrafe von höchstens 20 Jahren.

4.1 Verstöße durch Mitarbeiter

Alle Mitarbeiter und leitenden Angestellten des Unternehmens haben für die unverzügliche Einhaltung der einschlägigen Bestimmungen dieses Handbuchs zu sorgen. Verstößt ein Mitarbeiter oder eine Führungskraft gegen die in diesem Handbuch festgelegten Anforderungen, kann das Unternehmen nach eigenem Ermessen und in Abhängigkeit von bestimmten Faktoren (wie der Schwere und den Folgen des Verstoßes) Maßnahmen ergreifen, die unter anderem die Einleitung von Disziplinarverfahren und/oder die Meldung der Angelegenheit an die zuständigen Behörden umfassen.

5. Wichtige AML-CFT-Beauftragte

Es ist die Politik des Unternehmens, sicherzustellen, dass seine Geschäftstätigkeit in Übereinstimmung mit den geltenden gesetzlichen und aufsichtsrechtlichen Standards erfolgt. In seiner Eigenschaft als meldepflichtige Person muss das Unternehmen seine Verpflichtungen aus dem FIAMLA und dem FIAMLR einhalten.

Daher ernennt das Unternehmen einen Compliance-Beauftragten, einen MLRO und einen stellvertretenden MLRO und richtet Verfahren ein, die unter anderem Folgendes umfassen:

1. Identifizierung und Überprüfung der Identität von Kunden;
2. Sicherstellung einer ordnungsgemäßen Meldung verdächtiger Transaktionen;
3. Sicherstellung einer angemessenen Überprüfung von Kunden und potenziellen Mitarbeitern;
4. Unabhängige Audit-Funktion zur Prüfung des AML/CFT-Programms
5. Angemessene Schulung der Mitarbeiter zu AML/CFT; und
6. Aufrechterhaltung von Belegen für die Einhaltung der gesetzlichen und aufsichtsrechtlichen Anforderungen in Bezug auf AML-CFT.

5.1 Compliance-Beauftragter

Gemäß Vorschrift 22 (1) (a), 22 (2) und 22 (3) und den einschlägigen Bestimmungen des AML/CFT-Handbuchs ist das Unternehmen verpflichtet, einen Compliance-Beauftragten zu ernennen, der die in Absatz 5.1.1 unten beschriebenen Aufgaben hat. Das Unternehmen holt vor der Ernennung eines Compliance-Beauftragten die vorherige Genehmigung des FSC ein.

5.1.1 Aufgaben des Compliance-Beauftragten

Der Compliance-Beauftragte ist verantwortlich für:

a. Sicherstellung der kontinuierlichen Einhaltung der Anforderungen von FIAMLA und FIAMLR unter der ständigen Aufsicht des Verwaltungsrats und der Geschäftsleitung,
b. Übernahme der täglichen Verwaltung des AML-CFT-Programms der Gesellschaft,
c. Regelmäßige Berichterstattung an den Verwaltungsrat über den Stand der Einhaltung bzw. Nichteinhaltung der Vorschriften,
d. Mitwirkung an der Gestaltung, Umsetzung und Pflege der internen AML-CFT-Compliance-Handbücher, -Richtlinien und -Systeme des Unternehmens.

Mit anderen Worten und aus praktischer Sicht ist der Compliance-Beauftragte die zentrale Person, die für die Einhaltung von AML/CFT im Unternehmen verantwortlich ist.

Das Unternehmen stellt jederzeit sicher, dass der Compliance-Beauftragte:

a. zeitnahen und uneingeschränkten Zugang zu den Aufzeichnungen des Finanzinstituts hat;
b. über ausreichende Mittel zur Erfüllung seiner Aufgaben verfügt;
c. die volle Kooperation der Mitarbeiter des Finanzinstituts hat;
d. sich seiner Pflichten und der Pflichten des Finanzinstituts voll bewusst ist; und

e. berichtet direkt an den Verwaltungsrat und steht mit diesem in regelmäßigem Kontakt, so dass sich der Verwaltungsrat davon überzeugen kann, dass alle gesetzlichen Verpflichtungen und Bestimmungen des FIAMLA und der FIAML-Verordnungen 2018 sowie dieses Handbuchs eingehalten werden und dass das Finanzinstitut hinreichend solide Maßnahmen ergreift, um sich vor dem potenziellen Risiko, für Geldwäsche und Terrorismusfinanzierung missbraucht zu werden, zu schützen.

Darüber hinaus muss das Unternehmen vor seiner Ernennung die vorherige Genehmigung der FSC gemäß Abschnitt 24 des Financial Services Act 2007 einholen. Das Unternehmen stellt außerdem sicher, dass der Compliance-Beauftragte auch nach seiner Ernennung für diese Position geeignet und geeignet bleibt.

5.2 MLRO

Gemäß Vorschrift 26 (1) muss das Unternehmen einen MLRO ernennen, an den alle internen Meldungen verdächtiger Transaktionen zu richten sind, sowie einen stellvertretenden MLRO, der die Aufgaben des MLRO in dessen Abwesenheit wahrnimmt.

Im Einklang mit Vorschrift 26 (4) der FIAMLA-Verordnungen und den einschlägigen Bestimmungen der Leitlinien müssen der MLRO und der stellvertretende MLRO des Unternehmens:

1. eine ausreichend hohe Position in der Gesellschaft innehaben oder über ausreichende Erfahrung und Autorität verfügen, und
2. ein Recht auf direkten Zugang zum Verwaltungsrat der Gesellschaft haben und über genügend Zeit und Ressourcen verfügen, um seine Aufgaben wirksam zu erfüllen.

Ein und dieselbe Person kann zum MLRO und zum Compliance-Beauftragten ernannt werden, sofern (i) sie dies im Hinblick auf die jeweiligen Anforderungen der beiden Funktionen für angemessen hält und (ii) die zu ernennende Person über ausreichend Zeit und Ressourcen verfügt, um beide Funktionen wirksam auszuführen.

Sowohl der MLRO als auch der DMLRO sollten als aktive Nutzer auf der GoAML-Plattform der Financial Intelligence Unit (FIU) registriert sein, sobald sie in dieser Funktion zugelassen wurden und während ihrer gesamten Amtszeit.

5.2.1 Aufgaben der MLRO

Der MLRO muss Zugang zu allen relevanten Informationen oder Aufzeichnungen erhalten, um zu untersuchen, ob eine gemeldete Transaktion verdächtig ist oder nicht. Für die Zwecke der Untersuchung berücksichtigt der MLRO alle ihm zur Verfügung stehenden relevanten Informationen, um festzustellen, ob die gemeldete Transaktion verdächtig ist oder nicht. Der MLRO ist auch der zentrale Ansprechpartner für die FIU.

Der MLRO und der DMLRO werden auf der GoAML-Plattform der zentralen Meldestelle registriert, und die Nachweise für diese Registrierung werden aufbewahrt und der Aufsichtsbehörde auf Anfrage zur Verfügung gestellt.

Umgang mit Berichten über verdächtige Transaktionen

Sobald die MLRO oder die DMLRO einen internen STR erhält, nimmt sie einen Eintrag in das STR-Protokoll (siehe Anhang 3) mit allen Einzelheiten vor. Gemäß Regel 27 (e) muss die MLRO Zugang zu allen relevanten Informationen oder Aufzeichnungen erhalten, um zu beurteilen, ob die Transaktion verdächtig ist oder nicht.

Abschnitt 14(1) des FIAMLA sieht vor, dass die meldende Person eine Meldung über verdächtige Transaktionen (Suspicious Transaction Report, STR) an die FIU so bald wie möglich, spätestens **jedoch innerhalb von fünf Arbeitstagen** nach dem Tag, an dem sie von der verdächtigen Transaktion Kenntnis erlangt hat, zu erstatten hat. Der MLRO dokumentiert die Informationen, die zur Bewertung der gemeldeten Transaktion geprüft wurden. Gemäß Vorschrift 30 (3) muss das Datum, an dem die Meldung an die zentrale Meldestelle erfolgt ist, im Meldungsprotokoll festgehalten werden. In Fällen, in denen das Unternehmen dabei ist, eine STR-Meldung einzureichen, kann es die FIU um Rat fragen, wie mit dem Kunden zu verfahren ist oder ob die Transaktionen gestoppt werden können, ohne dass die FIU davon erfährt.

Kommt der MLRO nach der Prüfung zu dem Schluss, dass die gemeldete Transaktion nicht verdächtig ist, dokumentiert er die Informationen, die zur Bewertung der Transaktion geprüft wurden, sowie die Gründe für die Nichtmeldung an die FIU im STR-Protokoll. Zur Dokumentation der Informationen kann eine (physische oder elektronische) Akte angelegt werden, zu der nur der MLRO oder der stellvertretende MLRO Zugang hat und in der die folgenden Dokumente/Informationen festgehalten werden

a. Tatsachen, die sich auf die mutmaßliche verdächtige Aktivität/Transaktion beziehen
b. Dokumente/Vorkommnisse/Informationen im Zusammenhang mit der vom MLRO oder seinem Stellvertreter durchgeführten internen Untersuchung
c. Ergebnisse der internen Ermittlungen
d. Schriftliche Protokolle von Besprechungen mit Mitarbeitern während der internen Ermittlungen (falls vorhanden)
e. Schriftliche Analyse des MLRO / stellvertretenden MLRO zur Begründung der Entscheidung, eine STR bei der FIU einzureichen oder nicht einzureichen

Beachten Sie, dass die obige Liste nicht erschöpfend ist.

Der MLRO des Unternehmens sollte der Hauptkontaktpunkt des Unternehmens mit der FIU sein. Den leitenden Angestellten und Mitarbeitern des Unternehmens ist es strengstens untersagt, Informationen oder andere Angelegenheiten, die eine Untersuchung einer verdächtigen Transaktion beeinträchtigen könnten, an irgendeine Person weiterzugeben.

Alle Mitarbeiter sind über die Identität des Compliance Officers, des MLRO und des DMLRO zu unterrichten. Im Falle eines Wechsels des MLRO oder DMLRO sind die leitenden Angestellten und Mitarbeiter des Unternehmens entsprechend zu unterrichten. Der stellvertretende MLRO übernimmt die Pflichten und Verantwortlichkeiten des MLRO in Bezug auf die Meldung verdächtiger Transaktionen und erhält den gleichen Zugang zu Informationen und Unterlagen, damit er seine Aufgaben in Abwesenheit des MLRO wahrnehmen kann.

6. AML-CFT Risikobewertung

Section 17 des Financial Intelligence and Anti-Money Laundering Act 2002 ("FIAMLA") verpflichtet jede meldende Person, geeignete Schritte zu unternehmen, um die Risiken von Geldwäsche und Terrorismusfinanzierung für Kunden, Länder oder geografische Gebiete und Produkte, Dienstleistungen, Transaktionen oder Lieferkanäle zu ermitteln, zu bewerten und zu verstehen. Abschnitt 17 verpflichtet die Meldepflichtigen, alle relevanten Risikofaktoren zu berücksichtigen, bevor sie die Höhe des Gesamtrisikos, das geeignete Maß und die Art der anzuwendenden Risikominderung bestimmen. Art und Umfang der Bewertung müssen der Art und dem Umfang der Geschäftstätigkeit der berichtenden Person entsprechen und Folgendes berücksichtigen

a. alle relevanten Risikofaktoren, einschließlich
    i. die Art, den Umfang und die Komplexität der Tätigkeiten der berichtenden Person;
    ii. die von der berichtenden Person angebotenen Produkte und Dienstleistungen;
    iii. die Personen, für die die Produkte und Dienstleistungen erbracht werden, und die Art und Weise, in der sie erbracht werden;
    iv. die Art, den Umfang, die Komplexität und den Standort der Tätigkeiten des Kunden;
    v. die Abhängigkeit von Dritten in Bezug auf Elemente der Sorgfaltspflicht gegenüber Kunden; und
    vi. technologische Entwicklungen; und

b. das Ergebnis einer auf nationaler Ebene durchgeführten Risikobewertung und etwaige Leitlinien.

Gemäß Abschnitt 17 wird von den Meldepflichtigen auch erwartet, dass sie die Risiken der Geldwäsche oder der Terrorismusfinanzierung, die bei der Einführung eines neuen Produkts oder einer neuen Geschäftspraxis oder beim Einsatz einer neuen oder sich entwickelnden Technologie entstehen können, ermitteln und bewerten.

Gemäß § 17 FIAMLA ist eine Unternehmensrisikobewertung der Prozess, mit dem eine meldepflichtige Person feststellt und bewertet, wie anfällig sie für eine Verwicklung in Geldwäsche und Terrorismusfinanzierung ist, um geeignete Kontrollen und Maßnahmen zur Minimierung und Bewältigung dieser Risiken durchzuführen. Eine Bewertung des Geschäftsrisikos soll dem Meldepflichtigen dabei helfen, das Ausmaß zu ermitteln, in dem seine Geschäfte, Produkte und Dienstleistungen ML /TF ausgesetzt sind. Eine ordnungsgemäße Bewertung des Geschäftsrisikos sollte das Unternehmen in die Lage versetzen, sicherzustellen, dass sein AML-CFT-Rahmen den ML/TF-Risiken, denen es ausgesetzt ist, entspricht und auf diese ausgerichtet ist.

6.1 Bewertung von Geschäftsrisiken

Ziel der Bewertung des Geschäftsrisikos ist es, festzustellen, inwieweit die Geschäfte, Produkte und Dienstleistungen des Unternehmens ML /TF ausgesetzt sind. Gemäß Abschnitt 17 (2) des FIAMLA müssen bei der Bewertung des Geschäftsrisikos neben anderen Risikofaktoren sechs Schlüsselbereiche berücksichtigt werden:

a. die Art, den Umfang und die Komplexität der Tätigkeiten des Finanzinstituts;
b. die von dem Finanzinstitut angebotenen Produkte und Dienstleistungen;
c. die Personen, für die die Produkte und Dienstleistungen erbracht werden, und die Art und Weise, in der sie erbracht werden;
d. die Art, den Umfang, die Komplexität und den Standort der Geschäfte des Kunden;

e. die Abhängigkeit von Dritten in Bezug auf Elemente der Sorgfaltspflicht gegenüber dem Kunden; und
f. technologische Entwicklungen.

Darüber hinaus sind die Meldepflichtigen verpflichtet, die Ergebnisse der auf nationaler Ebene durchgeführten Risikobewertungen und etwaige Leitlinien zu berücksichtigen. Daher müssen die Ergebnisse des Berichts über die nationale Risikobewertung berücksichtigt werden.

6.1.1 Leitlinien zur Bewertung von Unternehmensrisiken

Daher ergreift das Unternehmen in seiner Eigenschaft als Berichtspflichtiger und damit als meldepflichtige Person geeignete Maßnahmen zur Durchführung einer Bewertung des Geschäftsrisikos, wie sie in Abschnitt 17 des FIAMLA vorgeschrieben ist.

Die Methodik für die Bewertung des Geschäftsrisikos ist in demselben Dokument enthalten wie die Bewertung des Geschäftsrisikos selbst. Wir bitten Sie, sich auf dieses Dokument zu beziehen (siehe Anhang 7).

Bei der Bewertung des Geschäftsrisikos sind die nachstehenden Risikofaktoren zu berücksichtigen:

1. Art, Umfang und Komplexität der Aktivitäten
    a. Überlegen Sie, welche Dienstleistungen das Unternehmen anbietet und wie diese Dienstleistungen für ML/TF missbraucht werden könnten.

    b. Aktive Einbeziehung aller Mitglieder der Geschäftsleitung in die Ermittlung der Risiken (Bedrohungen und Schwachstellen), die von ML/TF in den Bereichen ausgehen, für die sie verantwortlich sind.

    c. Berücksichtigung aller organisatorischen Faktoren, die das ML/TF-Risiko erhöhen können, z. B. Geschäftsvolumen und Outsourcing-Aspekte von regulierten Tätigkeiten oder Compliance-Funktionen.

    d. Berücksichtigung der Art, des Umfangs und der Komplexität der Geschäftstätigkeit, einschließlich der Vielfalt der Geschäfte, des Volumens und des Umfangs der Transaktionen sowie des Risikograds, der mit den einzelnen Geschäftsbereichen verbunden ist. Großvolumige und komplexere Transaktionen können ein höheres Geldwäscherisiko mit sich bringen als weniger komplexe und umfangreiche Transaktionen. Dies hängt jedoch auch von der Bewertung des Geschäftsfelds und der Art des Geschäfts ab. Um eine umfassendere Bewertung vornehmen zu können, müssen alle Faktoren zusammen betrachtet werden.

    e. Berücksichtigen Sie die Gerichtsbarkeiten, in denen das Unternehmen tätig ist, alle besonderen Bedrohungen, die von diesen Gerichtsbarkeiten ausgehen, und alle besonderen Schwachstellen innerhalb der Organisation in diesen Gerichtsbarkeiten. In Vorschrift 24(1) der FIAML-Verordnungen 2018 ist festgelegt, wie Drittländer mit hohem Risiko ermittelt werden sollten.

2. Art, Umfang und Komplexität der Aktivitäten

a. Überlegen Sie, welche Dienstleistungen das Unternehmen anbietet und wie diese Dienstleistungen für ML/TF missbraucht werden könnten.

b. Aktive Einbeziehung aller Mitglieder der Geschäftsleitung in die Ermittlung der Risiken (Bedrohungen und Schwachstellen), die von ML/TF in den Bereichen ausgehen, für die sie verantwortlich sind.

c. Berücksichtigung aller organisatorischen Faktoren, die das ML/TF-Risiko erhöhen können, z. B. Geschäftsvolumen und Outsourcing-Aspekte von regulierten Tätigkeiten oder Compliance-Funktionen.

d. Berücksichtigung der Art, des Umfangs und der Komplexität der Geschäftstätigkeit, einschließlich der Vielfalt der Geschäfte, des Volumens und des Umfangs der Transaktionen sowie des Risikograds, der mit den einzelnen Geschäftsbereichen verbunden ist. Großvolumige und komplexere Transaktionen können ein höheres Geldwäscherisiko mit sich bringen als weniger komplexe und umfangreiche Transaktionen. Dies hängt jedoch auch von der Bewertung des Geschäftsfelds und der Art des Geschäfts ab. Um eine umfassendere Bewertung vornehmen zu können, müssen alle Faktoren zusammen betrachtet werden.

e. Berücksichtigen Sie die Gerichtsbarkeiten, in denen das Unternehmen tätig ist, alle besonderen Bedrohungen, die von diesen Gerichtsbarkeiten ausgehen, und alle besonderen Schwachstellen innerhalb der Organisation in diesen Gerichtsbarkeiten. In Vorschrift 24(1) der FIAML-Verordnungen 2018 ist festgelegt, wie Drittländer mit hohem Risiko ermittelt werden sollten.

3. Von Finanzinstituten angebotene Produkte und Dienstleistungen
    a. Überlegen Sie, wie anfällig die angebotenen Dienstleistungen oder Produkte sind und wie sie für ML/TF missbraucht werden könnten. Bestimmte Merkmale der Produkte und ob es erhöhte Schwachstellen gibt, z. B. hohe Bargeldbeträge, virtuelle Währungen oder nicht zurückverfolgbare/anonyme Medien.

    b. Ob Zahlungen an unbekannte oder nicht verbundene Dritte erlaubt sind. Solche Zahlungen würden höhere Risiken mit sich bringen.

    c. Ob die Produkte/Dienstleistungen/Strukturen von besonderer oder ungewöhnlicher Komplexität sind.

4. Die Personen, denen die Produkte und Dienstleistungen zur Verfügung gestellt werden, und die Art und Weise, in der sie erbracht werden
    a. Berücksichtigen Sie die Bedrohungen, die von den verschiedenen Kundentypen ausgehen. Einige Beispiele sind politisch exponierte Personen ("PEPs"), sehr vermögende Personen, Personen, die aus einer Gerichtsbarkeit mit höherem Risiko stammen oder dort tätig sind, und Kunden, die nicht persönlich anwesend sind.

    b. Die Art des Produkts sollte berücksichtigt werden. Produkte oder Dienstleistungen mit höherem Risiko sind eher solche, die einen hohen Wert und ein hohes Volumen haben, bei denen unbegrenzt Gelder von Dritten entgegengenommen werden können und bei denen regelmäßig Gelder an Dritte gezahlt werden können, ohne dass eine CDD über die Dritten durchgeführt wird.

c. Die Geschwindigkeit, mit der Produkte und Dienstleistungen geliefert oder Transaktionen durchgeführt werden können.

d. Abschnitt 17A(b) FIAMLA schreibt vor, dass jede meldepflichtige Person die festgelegten Strategien, Kontrollen und Verfahren regelmäßig überprüfen, aktualisieren und gegebenenfalls verbessern muss. Daher ist die durchgeführte Unternehmensrisikobewertung mindestens jährlich zu überprüfen, um das Ausmaß der Exposition des Unternehmens gegenüber ML/TF-Risiken zu berücksichtigen.

5. Art, Umfang, Komplexität und Standort der Kundenaktivitäten
   a. ob der Kundenstamm in den Geschäftsbereichen tätig ist, die wahrscheinlich am anfälligsten für Korruption sind, z. B. Öl, Bauwesen oder Waffenhandel.

   b. Berücksichtigen Sie rechtliche Faktoren wie ein hohes Maß an organisierter Kriminalität, erhöhte Korruptionsanfälligkeit und unzureichende Rahmenbedingungen für die Verhinderung und Aufdeckung von Geldwäsche und Terrorismusfinanzierung in Ländern, in denen das Unternehmen möglicherweise Kunden hat.

   c. Die Länder, Territorien und geografischen Gebiete, zu denen die Kunden (und die wirtschaftlichen Eigentümer der Kunden) einen relevanten Bezug haben.

6.2 Bewertung des Kundenrisikos

Die mit einem Kunden verbundenen Risiken werden anhand der Bedeutung der Risikoindikatoren bestimmt. Gemäß § 17 Absatz 1 FIAMLA wird auf der Grundlage der gesammelten Identifizierungsdokumente und des Ergebnisses der Überprüfung eine GwG-Kundenrisikobewertung durchgeführt. Zu diesem Zweck wird eine Bewertung des Kundenrisikos unter Verwendung des Customer Risk Assessment Tool durchgeführt, um den Grad der mit der Geschäftstätigkeit mit dem Kunden verbundenen ML/TF-Risiken zu bestimmen. Wir bitten Sie, das Kundenrisikobewertungsinstrument entsprechend zu verwenden (siehe Anhang 8).

6.2.1 Prozess der Kundenrisikobewertung

Auf der Grundlage der bei der Identitätsüberprüfung gesammelten Informationen und der während der Interaktion mit dem Kunden erfassten Details muss der Benutzer des Kunden-Risiko-Bewertungs-Tools die Risiken durch Ausfüllen desselben bewerten.
Die Risikobewertungsstufen werden wie folgt kategorisiert:

Risikostufe	**Häufigkeit der Überprüfung**
Niedrig	Alle 3 Jahre
Mittel	Alle 2 Jahre

Hoch	Jährlich

Risikofaktoren

In der Risikobewertungsmatrix für Kunden wurden verschiedene Risikofaktoren berücksichtigt. Zum besseren Verständnis werden im Folgenden Hinweise gegeben (die auch Teil der verwendeten Risikobewertungsmethode sind):

Die grundlegenden Risikofaktorkategorien sind:

1. Kundenrisiken (Einzelpersonen/Unternehmen)
2. Geografische Risiken
3. Produkt-/Dienstleistungsrisiken

Kundenrisiken

Das Kundenrisiko ist mit allen Faktoren verbunden, die mit der Tätigkeit, dem Ruf, der Art oder dem Verhalten der Kunden zusammenhängen und die ML/TF-Risiken erhöhen könnten.

Bei der Ermittlung des mit Kunden verbundenen Risikos berücksichtigt das Unternehmen die geschäftliche oder berufliche Tätigkeit, den Ruf, die Struktur, die Art und das Verhalten des Kunden und des wirtschaftlichen Eigentümers des Kunden.

Risikofaktoren, die aufgrund der Kundenaktivität zu berücksichtigen sind **Aktivität**:

- ★ Hat der Kunde oder der wirtschaftliche Eigentümer Verbindungen zu Sektoren, die üblicherweise mit einem höheren Korruptionsrisiko verbunden sind, wie z. B. das Baugewerbe, die Pharmaindustrie, das Gesundheitswesen, der Waffenhandel und die Verteidigung, die mineralgewinnende Industrie oder das öffentliche Auftragswesen?
- ★ Bestehen zwischen dem Kunden oder dem wirtschaftlichen Eigentümer und Unternehmen Verbindungen zu Produkten oder Aktivitäten, die nach den Gesetzen oder Vorschriften des Aufnahmelandes oder nach internationalen Übereinkommen und Vereinbarungen als illegal gelten, einschließlich, aber nicht beschränkt auf die Anforderungen des Aufnahmelandes in Bezug auf Umwelt-, Gesundheits-, Sicherheits- und Arbeitsaspekte?
- ★ Hat der Kunde oder der wirtschaftliche Eigentümer direkte Verbindungen zu Unternehmen, die außerhalb der Risikobereitschaft des Unternehmens liegen? Steht er beispielsweise über eine Eigentumsstruktur oder eine Partnerschaft mit Kryptowährungsgeschäften in Verbindung, mit nicht lizenzierten Geschäften, die eine Lizenz erfordern, usw.
- ★ Hat der Kunde oder der wirtschaftliche Eigentümer Verbindungen zu Sektoren, die mit einem höheren ML/TF-Risiko verbunden sind, z. B. bestimmte Finanzinstitute, Glücksspiele, Wetten, Kasinos oder Devisenhandel?
- ★ Hat der Kunde oder der wirtschaftliche Eigentümer Verbindungen zu Geschäften, die mit erheblichen Bargeldbeträgen verbunden sind (Bargeld macht mehr als 30 % aller Transaktionen aus)?
- ★ Handelt es sich bei dem Kunden um eine juristische Person oder eine Rechtsvereinbarung, was ist der Zweck ihrer Niederlassung? Welcher Art ist zum Beispiel das Geschäft des Kunden?
- ★ Hat der Kunde politische Verbindungen, ist er beispielsweise eine politisch exponierte Person ("PEP") oder ist sein wirtschaftlicher Eigentümer ein PEP? Hat der Kunde oder der wirtschaftliche Eigentümer andere relevante Verbindungen zu einem PEP, z. B. PEPs aus der Verwandtschaft oder aus dem nahen Umfeld? Ist einer der Direktoren des Kunden ein PEP und, falls ja, üben diese PEPs eine wesentliche Kontrolle über den Kunden oder den wirtschaftlichen Eigentümer aus?

- ★ Unterliegt eine natürliche oder juristische Person durchsetzbaren Offenlegungspflichten, die sicherstellen, dass zuverlässige Informationen über den wirtschaftlichen Eigentümer des Kunden öffentlich zugänglich sind, z. B. börsennotierte Unternehmen, die eine solche Offenlegung zur Bedingung für die Börsennotierung machen?
- ★ Handelt es sich bei dem Kunden um ein auf eigene Rechnung handelndes Finanzinstitut aus einem Land mit wirksamen AML/CFT-Regelungen und wird es hinsichtlich der Einhaltung der lokalen AML/CFT-Verpflichtungen beaufsichtigt?
- ★ Gibt es Hinweise darauf, dass der Kunde in den letzten Jahren aufsichtsrechtlichen Sanktionen oder Durchsetzungsmaßnahmen wegen der Nichteinhaltung von AML/CFT-Verpflichtungen oder allgemeineren Verhaltensanforderungen unterworfen war?
- ★ Handelt es sich bei dem Kunden um eine öffentliche Verwaltung oder ein Unternehmen aus einem Land mit einem niedrigen, mittleren oder hohen Korruptionsniveau?
- ★ Stimmt der Hintergrund des Kunden oder des wirtschaftlichen Eigentümers mit dem überein, was das Unternehmen über die frühere, aktuelle oder geplante Geschäftstätigkeit, den Umsatz des Unternehmens, die Herkunft der Mittel und die Herkunft des Vermögens des Kunden oder des wirtschaftlichen Eigentümers weiß?
- ★ Wenn es sich bei dem Kunden um eine juristische Person handelt, deren Geschäftsprofil mit Geld zu tun hat, verfügen die Unternehmen über ausreichende AML/CTF-Richtlinien und -Verfahren, um ihre eigenen Kunden zu überwachen.

Risikofaktoren, die aufgrund der **Reputation** der Kunden zu berücksichtigen sind:

- ★ Gibt es negative Medienberichte oder andere relevante Informationsquellen über den Kunden, z. B. Vorwürfe von Kriminalität, Bestechung, Terrorismus und anderen Finanzdelikten gegen den Kunden oder den wirtschaftlichen Eigentümer? Wenn ja, sind diese Quellen zuverlässig und glaubwürdig? Das Unternehmen sollte die Glaubwürdigkeit der Anschuldigungen u. a. anhand der Qualität und Unabhängigkeit der Datenquelle und der Beständigkeit der Berichterstattung über diese Anschuldigungen beurteilen. Die Tatsache, dass keine strafrechtlichen Verurteilungen vorliegen, reicht nicht aus, um den Vorwurf des Fehlverhaltens zurückzuweisen.
- ★ Wurden die Vermögenswerte des Kunden, des wirtschaftlichen Eigentümers oder einer Person, von der öffentlich bekannt ist, dass sie in enger Beziehung zu ihr steht, aufgrund von Verwaltungs- oder Strafverfahren oder aufgrund von Vorwürfen des Terrorismus oder der Terrorismusfinanzierung eingefroren? Hat das Unternehmen begründeten Anlass zu der Vermutung, dass der Kunde oder der wirtschaftliche Eigentümer oder eine Person, von der öffentlich bekannt ist, dass sie in enger Beziehung zu ihr steht, zu irgendeinem Zeitpunkt in der Vergangenheit von einem solchen Einfrieren von Vermögenswerten betroffen war?
- ★ War der Kunde oder der wirtschaftliche Eigentümer in der Vergangenheit Gegenstand einer Meldung über verdächtige Transaktionen?
- ★ Gab es interne Informationen über die Integrität des Kunden oder des wirtschaftlichen Eigentümers, die z. B. im Rahmen einer langjährigen Geschäftsbeziehung gewonnen wurden?
- ★ Gibt es andere Verhaltensauffälligkeiten des Kunden, wie z. B. die mangelnde Bereitschaft, falsche Unternehmensinformationen oder -unterlagen zur Verfügung zu stellen?

Risikofaktoren, die aufgrund der **Art und des Verhaltens** der Kunden zu berücksichtigen sind:

- ★ Hat der Kunde berechtigte Gründe, seine Identität nicht stichhaltig nachweisen zu können, etwa weil er Asylbewerber ist?
- ★ Bestehen Zweifel an der Wahrhaftigkeit oder Richtigkeit der Identität des Kunden oder des wirtschaftlichen Eigentümers?

- ★ Gibt es Anzeichen dafür, dass der Kunde versuchen könnte, die Aufnahme einer Geschäftsbeziehung zu vermeiden? Beabsichtigt der Kunde beispielsweise, eine Transaktion oder mehrere einmalige Transaktionen durchzuführen, bei denen die Aufnahme einer Geschäftsbeziehung wirtschaftlich sinnvoller wäre?
- ★ Ist die Eigentums- und Kontrollstruktur des Kunden transparent und sinnvoll? Wenn die Eigentums- und Kontrollstruktur des Kunden komplex oder undurchsichtig ist, gibt es dann einen offensichtlichen wirtschaftlichen oder rechtlichen Grund?
- ★ Gibt der Kunde Inhaberaktien aus?
- ★ Hat der Kunde Nominee-Aktionäre?
- ★ Handelt es sich bei dem Kunden um eine juristische Person oder um eine Vereinbarung, die als Vehikel zum Halten von Vermögenswerten genutzt werden könnte?
- ★ Gibt es einen triftigen Grund für Änderungen in der Eigentums- und Kontrollstruktur des Kunden?
- ★ Stimmen die vom Kunden bereitgestellten Informationen und Unterlagen mit Informationen aus einer unabhängigen öffentlichen Quelle überein?
- ★ Verlangt der Kunde ein unnötiges oder unangemessenes Maß an Geheimhaltung? Ist der Kunde beispielsweise nicht bereit, CDD-Informationen (Name des Kunden, Foto auf einem offiziellen Dokument und Wohnanschrift) weiterzugeben, oder scheint er die wahre Natur seines Geschäfts verschleiern zu wollen?
- ★ Lässt sich die Herkunft des Vermögens oder der Mittel des Kunden, des wirtschaftlichen Eigentümers oder der juristischen Person leicht erklären, z. B. durch Beruf, Erbschaft, Finanzunterlagen oder Investitionen? Ist die Erklärung plausibel?
- ★ Nutzt der Kunde die Produkte und Dienstleistungen, die er in Anspruch genommen hat, wie bei Aufnahme der Geschäftsbeziehung erwartet?
- ★ Könnte der Kunde, wenn er nicht im Lande ansässig ist, seine Bedürfnisse anderswo besser befriedigen? Gibt es eine solide wirtschaftliche und rechtliche Begründung dafür, dass der Kunde die gewünschte Art von Finanzdienstleistung nachfragt?
- ★ Ist öffentlich bekannt, dass dem Kundenunternehmen Bußgelder angedroht wurden. Wenn ja, standen die Bußgelder/Warnungen im Zusammenhang mit Finanzkriminalität/Terrorismusfinanzierung? Gab es einen möglichen Zusammenhang mit kriminellen Aktivitäten oder handelte es sich lediglich um einen unbeabsichtigten Rechtsverstoß? Wie hat sich das Unternehmen verhalten? Welche weiteren Maßnahmen/Reaktionen hat das Unternehmen nach Erhalt der Verwarnungen/Bußgelder ergriffen? Wurden z. B. die bereitgestellten Empfehlungen zur Erfüllung der rechtlichen Anforderungen akzeptiert und befolgt?
- ★ Ist die offizielle Website des Kunden aktiv und sieht entsprechend der Art der Geschäftstätigkeit des Kunden legitim aus?

Possible factors that the Company uses/implements to mitigate risk the risk for e-money products:

- ★ Um finanzielle oder rufschädigende Schäden zu vermeiden, die dem Unternehmen möglicherweise durch seine Kunden entstehen, durchläuft jeder neue Kunde (natürliche oder juristische Person) mehrere Stufen von Schutzmaßnahmen. Angefangen bei der elektronischen Identifizierung und der Einreichung von Dokumenten werden alle Kundeninformationen sorgfältig im Rahmen des CDD-Verfahrens und des Abgleichs der Kundeninformationen mit PEP-/Sanktionslisten, der Suche nach unerwünschten Medien, der Bewertung des Kundenrisikos durch einen AML-Spezialisten und einer zweiten Überprüfungsstufe durch den MLRO überprüft, bevor einem Kunden der Zugang zu den Systemen des Unternehmens gewährt wird. Nachdem der Kunde entsprechend der ihm zugewiesenen Risikokategorie aufgenommen wurde, werden seine KYC-Daten und -Aktivitäten in regelmäßigen Abständen (niedrig - alle 3 Jahre, mittel - alle 2 Jahre, hoch - alle 1 Jahr oder weniger) von AML-Spezialisten bewertet, und je nach den

erhaltenen Ergebnissen werden bestimmte Maßnahmen ergriffen (z. B. KYC-Aktualisierungen, Anforderung von Erklärungen für den Kunden, Entfernung des Kunden aus dem System); außerdem werden die Kundeninformationen täglich mit Sanktions- und PEP-Listen abgeglichen;

- ★ Als Teil des CDD-Verfahrens während des Kundenanbahnungsprozesses ist es für jeden potenziellen Kunden aus dem Finanzsektor obligatorisch, das Vorhandensein wirksamer AML-Prozesse und -Verfahren für seine Kunden nachzuweisen und zu belegen;
- ★ Korrekte Regeln für das System zur Überwachung von Kundentransaktionen, die eine Änderung der Kundenaktivität oder ein unerwartetes Verhalten auslösen (plötzliche Nutzung von Produkten wie Prepaid-Karten im Ausland, Transaktionen in beträchtlicher Höhe, die knapp unter dem Schwellenwert liegen, Transaktionen mit hohen Beträgen, Transaktionen, die von vielen verschiedenen Konten stammen oder an viele verschiedene Konten gesendet werden usw.) und Warnmeldungen erzeugen;

Häufig werden Änderungen der persönlichen Daten des Kunden (Identifikation, verknüpfte Bankkonten) wie auch andere Änderungen der Kundeninformationen aufgezeichnet, und Prüfpfade mit Informationen über die erwähnten Änderungen sind für AML-Spezialisten, die regelmäßige Kundenüberprüfungen durchführen, sichtbar. Wenn sich die Änderungen signifikant häufen, können die Kunden kontaktiert und um eine Aktualisierung des KYC-Profils gebeten werden.

Geografische Risiken

Das Länderrisiko bezieht sich auf alle geografischen Standorte, Gerichtsbarkeiten oder Beziehungen zu Gerichtsbarkeiten, die ein ML/TF-Risiko darstellen können.

- ★ Bei der Ermittlung der mit Ländern und geografischen Gebieten verbundenen Risiken berücksichtigt das Unternehmen die Gerichtsbarkeiten, in denen der Kunde und der wirtschaftliche Eigentümer ansässig sind, die Orte, an denen Geschäfte getätigt werden, Zugehörigkeiten, andere relevante persönliche Verbindungen, Informationen aus öffentlichen Quellen über die Gerichtsbarkeiten, in denen in jüngster Zeit Vorfälle im Zusammenhang mit jeglicher Art von Finanzkriminalität, Terrorismus, Bestechung und Korruption stattgefunden haben. Das Unternehmen verfügt über seine eigenen internen Länderrisikobewertungen, die auf der Grundlage mehrerer zuverlässiger und glaubwürdiger Quellen (Wolfsberg, FATF, Country Corruption Index, TF-Index, KYC usw.) erstellt wurden. Gemäß diesen Bewertungen werden alle genannten Risiken auf der Grundlage der Rechtsprechung (Geldwäsche, Terrorismusfinanzierung, Bestechung/Korruption/Steuervermeidung) in die Sorgfaltspflichten für Kunden aufgenommen.

Bei der Bewertung der Risiken sind allgemeine Regeln zu beachten:

- ★ Wenn die in der Geschäftsbeziehung verwendeten Gelder im Ausland generiert wurden, sind das Ausmaß der Vortaten zur Geldwäsche und die Wirksamkeit des Rechtssystems eines Landes besonders relevant;
- ★ Wenn Gelder aus Ländern eingehen oder dorthin gesendet werden, in denen bekanntermaßen terroristische Gruppen operieren, prüft das Unternehmen, inwieweit dies auf der Grundlage seiner Kenntnisse über den Zweck und die Art der Geschäftsbeziehung zu erwarten ist oder einen Verdacht erregen könnte;
- ★ Handelt es sich bei dem Kunden um ein Kredit- oder Finanzinstitut, achtet das Unternehmen besonders auf die Angemessenheit der AML/CFT-Regelung des Landes und die Wirksamkeit der AML/CFT-Aufsicht;
- ★ Handelt es sich bei dem Kunden um ein Unternehmen/eine juristische Person oder einen Trust, berücksichtigt das Unternehmen, inwieweit das Land, in dem der Kunde und gegebenenfalls der wirtschaftliche Eigentümer registriert sind, die internationalen Steuertransparenzstandards tatsächlich einhält.

Risikofaktoren, die je nach **Gerichtsbarkeit** zu berücksichtigen sind.

★ Bei der Ermittlung der Wirksamkeit der AML/CFT-Verpflichtungen eines Landes:
- Wurde festgestellt, dass das Land strategische Defizite bei der Erfüllung seiner AML/CFT-Verpflichtungen aufweist (Drittland mit hohem Risiko)?
- Gibt es Informationen aus mehr als einer glaubwürdigen und verlässlichen Quelle über die Qualität der AML/CFT-Kontrollen des Landes, einschließlich Informationen über die Qualität und Effektivität der regulatorischen Durchsetzung und Aufsicht? Beispiele für mögliche Quellen sind gegenseitige Evaluierungsberichte der Financial Action Task Force (FATF) oder regionaler Gremien nach Art der FATF (ein guter Ausgangspunkt ist eine Zusammenfassung und die wichtigsten Ergebnisse sowie die Bewertung der Einhaltung der Empfehlungen 10 (Sorgfaltspflicht gegenüber Kunden und Aufbewahrung von Unterlagen), 26 (Regulierung und Beaufsichtigung von Finanzinstituten), 27 (Befugnisse der Aufsichtsbehörden) und die unmittelbaren Ergebnisse 3 (Aufsicht) und 4 (Präventivmaßnahmen) der FATF-Liste der mit hohem Risiko behafteten und nicht kooperativen Länder, Bewertungen des Internationalen Währungsfonds (IWF) und Berichte des Programms zur Bewertung des Finanzsektors (FSAP). Die Mitgliedschaft in der FATF oder einem FSRB (z. B. MoneyVal) bedeutet nicht, dass die AML/CFT-Regelung des Landes angemessen und wirksam ist.

★ Bei der Ermittlung des Risikos der Terrorismusfinanzierung in einem Land:
- Gibt es Informationen, z. B. von Strafverfolgungsbehörden oder glaubwürdigen und verlässlichen offenen Medienquellen, die darauf hindeuten, dass ein Land terroristische Aktivitäten finanziert oder unterstützt oder dass Gruppen, die terroristische Straftaten begehen, bekanntermaßen in dem Land oder Gebiet tätig sind?
- Unterliegt das Land Finanzsanktionen, Embargos oder Maßnahmen im Zusammenhang mit Terrorismus, Terrorismusfinanzierung oder Proliferation, die z. B. von den Vereinten Nationen oder der Europäischen Union verhängt wurden.

★ Bei der Ermittlung des Niveaus der Transparenz und der Einhaltung der Steuervorschriften in einem Land:
- Gibt es Informationen aus mehr als einer glaubwürdigen und zuverlässigen Quelle, dass das Land als konform mit den internationalen Standards für Steuertransparenz und Informationsaustausch eingestuft wurde? Gibt es Belege dafür, dass die einschlägigen Vorschriften in der Praxis tatsächlich umgesetzt werden? Beispiele für mögliche Quellen sind Berichte des Global Forum on Transparency and the Exchange of Information for Tax Purposes (Globales Forum für Transparenz und Informationsaustausch für Steuerzwecke) der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD), in denen Länder im Hinblick auf Steuertransparenz und Informationsaustausch bewertet werden; Bewertungen der Verpflichtung des Landes zum automatischen Informationsaustausch auf der Grundlage des Common Reporting Standard; Bewertungen der Einhaltung der FATF-Empfehlungen 9 (Geheimhaltungsvorschriften für Finanzinstitute), 24 (Transparenz und wirtschaftliches Eigentum an juristischen Personen) und 25 (Transparenz und wirtschaftliches Eigentum an Rechtsvereinbarungen) sowie der unmittelbaren Ergebnisse 2 (internationale Zusammenarbeit) und 5 (juristische Personen und Rechtsvereinbarungen) durch die FATF oder die FSRBs; und Bewertungen des IWF (z. B. z. B. IWF-Bewertungen von Offshore-Finanzzentren).
- Hat sich das Land auf den gemeinsamen Meldestandard für den automatischen Informationsaustausch, den die G20 im Jahr 2014 angenommen hat, verpflichtet und diesen tatsächlich umgesetzt?
- Hat das Land verlässliche und zugängliche Register der wirtschaftlichen Eigentümer eingerichtet?

★ Bei der Ermittlung des Risikos im Zusammenhang mit der Höhe der Vortaten zur Geldwäsche:

- Gibt es Informationen aus glaubwürdigen und verlässlichen öffentlichen Quellen über das Ausmaß von Vortaten zur Geldwäsche, z. B. Korruption, organisierte Kriminalität, Steuerkriminalität und schwerer Betrug? Beispiele sind Korruptionswahrnehmungsindizes, OECD-Länderberichte über die Umsetzung des OECD-Übereinkommens zur Bekämpfung von Bestechung und der Weltdrogenbericht des Büros der Vereinten Nationen für Drogen- und Verbrechensbekämpfung.
- Gibt es Informationen aus mehr als einer glaubwürdigen und zuverlässigen Quelle über die Fähigkeit des Ermittlungs- und Justizsystems des betreffenden Landes, diese Straftaten wirksam zu untersuchen und zu verfolgen?

Mögliche Faktoren, die in DER FIRMA eingesetzt werden, um das Risiko für E-Geld-Produkte zu mindern:

★ Das Unternehmen achtet besonders auf Länder, von denen bekannt ist, dass sie terroristische Aktivitäten finanzieren oder unterstützen oder in denen Gruppen, die terroristische Straftaten begehen, aktiv sind, sowie auf Länder, gegen die Finanzsanktionen, Embargos oder Maßnahmen im Zusammenhang mit Terrorismus, Terrorismusfinanzierung oder Proliferation verhängt wurden.

★ Der Kunde muss ein Dokument vorlegen, das seine Staatsangehörigkeit und seinen Wohnsitz sowie den Ort seiner Niederlassung und seiner Geschäftstätigkeit während des Onboarding-Verfahrens nachweist, um das Risiko zu mindern, das sich aus einer möglichen Zugehörigkeit zu einem potenziell schädlichen Land ergibt.

Produkte/Dienstleistungen Risken

Das Produkt-, Dienstleistungs- und Transaktionsrisiko bezieht sich auf alle Produkte, Dienstleistungen und Transaktionen, die Bedingungen für das Auftreten von Geldwäsche-/Transaktionsrisiken schaffen könnten.

Bei der Ermittlung des mit Produkten, Dienstleistungen und Transaktionen verbundenen Risikos berücksichtigt das Unternehmen hauptsächlich die unten aufgeführten Faktoren:

★ der Grad der Transparenz oder Undurchsichtigkeit, den das Produkt, die Dienstleistung oder die Transaktion bietet;
★ die Komplexität des Produkts, der Dienstleistung oder des Geschäfts;
★ der Wert oder Umfang des Produkts, der Dienstleistung oder der Transaktion.

Für E-Geld-Produkte:

★ Schwellenwerte;
★ die Finanzierungsmethode;
★ Nützlichkeit und Verhandelbarkeit.

Risikofaktoren, die aufgrund der **Transparenz** zu berücksichtigen sind:

★ Inwieweit ermöglichen Produkte oder Dienstleistungen dem Kunden, dem wirtschaftlichen Eigentümer oder den Begünstigtenstrukturen, anonym zu bleiben oder ihre Identität zu verbergen? Beispiele für solche Produkte und Dienstleistungen sind Inhaberaktien, Treuhandanlagen, Offshore-Vehikel und bestimmte Trusts sowie juristische Personen wie Stiftungen, die so strukturiert werden können, dass sie die Anonymität nutzen und Geschäfte mit Briefkastenfirmen oder Unternehmen mit nominierten Aktionären ermöglichen;
★ Inwieweit ist es möglich, dass ein Dritter, der nicht an der Geschäftsbeziehung beteiligt ist, Anweisungen erteilt?

Risikofaktoren, die aufgrund der **Komplexität** zu berücksichtigen sind:

- ★ Inwieweit ist die Transaktion komplex und betrifft sie mehrere Parteien oder mehrere Gerichtsbarkeiten, z. B. bei bestimmten Handelsfinanzierungsgeschäften? Handelt es sich um einfache Transaktionen, z. B. regelmäßige Zahlungen an Unternehmenslieferanten für bereitgestellte Materialien?
- ★ Inwieweit erlauben Produkte oder Dienstleistungen Zahlungen von Dritten oder akzeptieren Überzahlungen, wo dies normalerweise nicht zu erwarten wäre? Wenn Zahlungen von Dritten erwartet werden, ist dem Unternehmen die Identität des Dritten bekannt, z. B. ob es sich um eine staatliche Leistungsbehörde oder einen Bürgen handelt? Oder werden Produkte und Dienstleistungen ausschließlich durch Überweisungen vom eigenen Konto des Kunden bei einem anderen Finanzinstitut finanziert?
- ★ Kennt das Unternehmen die Risiken, die mit seinem neuen oder innovativen Produkt oder seiner Dienstleistung verbunden sind, insbesondere wenn es sich um den Einsatz neuer Technologien oder Zahlungsmittel handelt?

Risikofaktoren, die je nach **Wert oder Größe** zu berücksichtigen sind:

- ★ Inwieweit sind Produkte oder Dienstleistungen bargeldintensiv?
- ★ Inwieweit erleichtern oder fördern die Produkte oder Dienstleistungen Transaktionen mit hohem Wert? Gibt es Obergrenzen für den Transaktionswert oder die Höhe der Prämie, die die Nutzung des Produkts oder der Dienstleistung für ML/TF-Zwecke einschränken könnten?

Mögliche Faktoren, die im Unternehmen zur Abschwächung des Risikos eingesetzt werden.

- ★ Schwellenwerte: das Produkt
    - setzt Kleinbetragsgrenzen für Zahlungen, Aufladungen oder Rücknahmen, einschließlich Barabhebungen (obwohl ein niedriger Schwellenwert allein möglicherweise nicht ausreicht, um das TF-Risiko zu verringern);
    - die Anzahl der Zahlungen, Aufladungen oder Rückzahlungen, einschließlich Bargeldabhebungen, in einem bestimmten Zeitraum begrenzt;
    - Begrenzung des Geldbetrags, der auf dem E-Geld-Produkt/Konto zu einem bestimmten Zeitpunkt gespeichert werden kann.

- ★ Finanzierung: das Produkt
    - verlangt, dass die Mittel für den Kauf oder das Aufladen nachweislich von einem Konto abgehoben werden, das auf den alleinigen oder gemeinsamen Namen des Kunden bei einem Kredit- oder Finanzinstitut im EWR geführt wird;

7. Sorgfaltspflicht gegenüber Kunden

Generell gilt, dass das Unternehmen bei potenziellen Kunden/Kundinnen die normale Sorgfaltspflicht anwendet oder im Falle von Kundenbeziehungen mit hohem Risiko verstärkte Sorgfaltsmaßnahmen ergreift. Besteht ein geringes Geldwäscherisiko, kann das Unternehmen eine vereinfachte Sorgfaltspflicht anwenden, wie unten beschrieben.

Vereinfachte Sorgfaltspflicht

Die Anwendung vereinfachter Sorgfaltspflichten bedeutet nicht den Verzicht auf CDD-Maßnahmen, sondern vielmehr die Anwendung reduzierter Maßnahmen, die dem vom Kunden oder der spezifischen Situation ausgehenden Risiko angemessen sein müssen.

Beschließt ein Finanzinstitut, die vereinfachten Maßnahmen in Bezug auf einen bestimmten Antragsteller anzuwenden, so muss es:

1. diese Entscheidung in einer Weise dokumentieren, die die Faktoren, die es berücksichtigt hat (einschließlich der Aufbewahrung aller einschlägigen Belege), und seine Gründe für die Annahme der betreffenden Maßnahmen erläutert; und
2. die Beziehung zu dem Antragsteller (einschließlich der Frage, ob die vereinfachten Maßnahmen weiterhin angemessen sind) ständig überprüfen und zu diesem Zweck geeignete Strategien, Verfahren und Kontrollen anwenden.

Vereinfachte CDD-Maßnahmen finden in keinem Fall Anwendung, wenn ein Finanzinstitut weiß, vermutet oder berechtigten Grund zu der Annahme hat, dass ein Kunde oder ein Antragsteller in Geldwäsche oder Terrorismusfinanzierung verwickelt ist oder dass die von dem Kunden oder Antragsteller durchgeführte Transaktion im Namen einer anderen in Geldwäsche verwickelten Person durchgeführt wird, oder wenn andere Indikatoren für ein Geldwäsche- oder Terrorismusrisiko vorliegen. Werden vereinfachte CDD-Maßnahmen eingeführt, sollten die Finanzinstitute einen risikobasierten Ansatz anwenden, um zu entscheiden, ob sie die vereinfachten CDD-Maßnahmen in einer bestimmten Situation anwenden und/oder mit den vereinfachten Maßnahmen fortfahren, obwohl die Konten dieser Kunden weiterhin der Transaktionsüberwachungspflicht unterliegen.

7.1 Identitätsüberprüfung

Das Unternehmen ist gesetzlich verpflichtet, seine Kunden zu identifizieren, unabhängig davon, ob es sich um ständige oder gelegentliche Kunden handelt, und die Identität seiner Kunden anhand zuverlässiger, unabhängiger Quelldokumente, Daten oder Informationen zu überprüfen, die von der Aufsichtsbehörde vorgegeben werden. Mit anderen Worten geht es bei der Identitätsprüfung darum, sicherzustellen, dass die Kunden die sind, die sie vorgeben zu sein.

Die Standarddokumente, die von Kunden zur Identitätsüberprüfung verlangt werden, sind in den Tabellen 1 bis 3 aufgeführt. Das Sammeln der erforderlichen Informationen anhand der angegebenen Dokumente ermöglicht es dem Unternehmen,:

1. ein Profil des Kunden zu erstellen,
2. das mit dem Kunden verbundene ML/TF-Risiko zu bewerten,
3. auf der Grundlage des Profils und der Risikobewertung des Kunden zu entscheiden, ob es eine Geschäftsbeziehung mit ihm eingehen möchte oder nicht.

7.1.1 Einzelpersonen

Wird die Geschäftsbeziehung zwischen der Gesellschaft und einer in eigenem Namen handelnden natürlichen Person aufgenommen, sind die in Tabelle 1 aufgeführten Unterlagen vom Kunden anzufordern, um die Bestimmungen der Verordnung 4 zu erfüllen:

Tabelle 1 - Von Kunden anzufordernde Dokumente - Einzelpersonen

Erforderliche Informationen	Quelldokument	Einzelheiten
• Vollständiger Name (einschließlich früherer Namen) • Datum und Ort der Geburt, • Staatsangehörigkeit, • Geschlecht • Von der Regierung vergebene persönliche Identifikationsnummer oder andere von der Regierung vergebene eindeutige Kennung	• Nationale Identitätskarte, oder • Aktueller gültiger Reisepass, • Ein offizielles Dokument, das die Namensänderung belegt (z. B. eine Heiratsurkunde, eine Bescheinigung über die Namensänderung),	Der Reisepass oder Personalausweis sollte mit einem Foto und der Unterschrift der Person versehen sein. Wenn der Kunde mehr als eine Staatsangehörigkeit besitzt, sollten Pässe oder nationale Ausweisdokumente für die zusätzliche Staatsangehörigkeit angefordert werden.
• Aktuelle und ständige Adresse	• Eine Rechnung eines Versorgungsunternehmens (Festnetztelefonrechnung/Gasrechnung/Stromrechnung/Wasserrechnung), die innerhalb der letzten 3 Monate ausgestellt wurde, oder • ein Kontoauszug, der innerhalb der letzten 3 Monate ausgestellt wurde, oder • eine Kreditkartenabrechnung, die innerhalb der letzten 3 Monate ausgestellt wurde, oder • ein Schreiben einer professionellen Person, z. B. eines Rechtsanwalts, eines Wirtschaftsprüfers, eines Bankiers oder eines Notars, die die Person kennt. Das Schreiben sollte die ständige Wohnanschrift der Person enthalten.	Postfachadressen gelten nicht als ständige Wohnanschrift und können nicht akzeptiert werden. Rechnungen von Versorgungsunternehmen sollten auf den Namen des Kunden lauten. Wenn das Dokument auf den Namen eines Elternteils (Mutter oder Vater) lautet, sollte die Geburtsurkunde des Kunden vorgelegt werden. Wenn die Stromrechnung auf den Namen eines Dritten lautet, ist ein Schreiben des Dritten vorzulegen, in dem bestätigt wird, dass der Kunde an der auf der Stromrechnung angegebenen Adresse wohnt, und eine beglaubigte Kopie des Personalausweises des Dritten ist vorzulegen.
• Beruf und Name des Arbeitgebers	• Berufsbezeichnung und Name des Arbeitgebers, oder • Lebenslauf, oder	Bei Selbstständigen: Gewerbeschein und Gewerbeanmeldung. Der Zeitraum (d. h. die Daten) der

	• Informationen zum beruflichen Hintergrund • Art und Einzelheiten der selbständigen Tätigkeit, falls zutreffend. • Bei Selbstständigen: Gewerbeschein und Gewerbeanmeldung.	Beschäftigung und der Name des Arbeitgebers sollten im Lebenslauf angegeben werden. Alternativ können die Angaben zum beruflichen Hintergrund auch während der Kundenregistrierung erfasst werden.
• Quelle der Mittel, die der Kunde zur Finanzierung des Erwerbs oder der Miete verwenden will	• Relevante Nachweise (falls zutreffend).	All fields of the form should be completed. The form should be signed and dated by the client. Alternatively, source of funds information may be requested during the registration process.

7.1.2 Juristische Personen oder Rechtsvereinbarungen

Wird die Geschäftsbeziehung zwischen dem Unternehmen und einer juristischen Person oder Rechtsvereinbarung aufgenommen, ist das Unternehmen bei Annahme des Angebots durch den Kunden verpflichtet, Folgendes zu überprüfen:

1. Den Namen, die Rechtsform und den Nachweis der Existenz des Kunden;
2. die Befugnisse, die den Kunden regeln und binden (d.h. wer den Kunden leitet und wer das Recht hat, ihn zu vertreten und in seinem Namen zu unterzeichnen);
3. die Namen der Personen, die bei dem Kunden leitende Positionen innehaben, und
4. die Adresse des eingetragenen Sitzes oder der Hauptniederlassung des Kunden.

Das Unternehmen sollte auch die Art der Geschäftstätigkeit und die Eigentümerstruktur eines Kunden, bei dem es sich um eine juristische Person oder Rechtsform handelt, kennen und dokumentieren.

Daher müssen die in Tabelle 2 aufgeführten Dokumente zur Identitätsprüfung vom Kunden angefordert werden.

In Tabelle 2 sind die Standarddokumente zur Identitätsprüfung aufgeführt, die von Kunden im Allgemeinen verlangt werden. Bei der Aufnahme eines neuen Kunden wird dieser aufgefordert, die Allgemeinen Geschäftsbedingungen auszufüllen und zu unterzeichnen sowie die auf der Website geforderten KYC-Informationen und Dokumente einzureichen.

Tabelle 2 - Von Kunden anzufordernde Dokumente - Juristische Personen oder Rechtsvereinbarungen

Art der juristischen Person/Rechtsvereinbarung	**Anzuforderndes Dokument**
Unternehmen	• Bescheinigung über die Eintragung oder Registrierung, • Gesellschaftsvertrag und Satzung oder Verfassung (je nach Fall), • Suche im Unternehmensregister

	• Unbedenklichkeitsbescheinigung einer zuständigen nationalen Stelle, • Unternehmensregistrierungskarte (falls zutreffend), • Übersicht über die Aktionärsstruktur bis hin zum wirtschaftlichen Eigentümer, • Letztes Register der Direktoren, • Letztes Register der Mitglieder/Aktionäre, • Adresse des eingetragenen Firmensitzes und des Hauptgeschäftssitzes (falls abweichend vom eingetragenen Firmensitz), • Letzter geprüfter Jahresabschluss oder Jahresbericht, falls verfügbar, • Dokumente zur Überprüfung der Identität der Geschäftsführer, der Hauptaktionäre und des wirtschaftlichen Eigentümers, • Identitätsnachweis und Wohnanschrift der Personen, die bevollmächtigt sind, das Unternehmen für die Zwecke der Transaktion zu vertreten und die erforderlichen Dokumente zu unterzeichnen
Personengesellschaft	• Gesellschaftsvertrag oder Gesellschaftsurkunde, • Bescheinigung über die Eintragung der Partnerschaft, falls sie eingetragen ist, • Nachweis, dass die Partnerschaft weiterhin besteht (Unbedenklichkeitsbescheinigung des Registerführers) • Letzter geprüfter Jahresabschluss oder Jahresbericht, • Identitätsnachweis für den geschäftsführenden/komplementären Gesellschafter, • Letztes Register (oder gleichwertiges Dokument), das die Namen, Adressen und prozentualen Anteile der Kommanditisten zeigt, • Adresse des eingetragenen Firmensitzes und des Hauptgeschäftssitzes (falls abweichend vom eingetragenen Firmensitz), • Dokumente zur Identitätsprüfung der Kommanditisten und des wirtschaftlichen Eigentümers, • Identitätsnachweis und Wohnanschrift der Personen, die bevollmächtigt sind, die Gesellschaft für die Zwecke der Transaktion zu vertreten und die Dokumente zu unterzeichnen, und
Sozietät	• Acte de société oder ein gleichwertiges Dokument zur Gründung der Societé, • Wenn die Gesellschaft eingetragen ist, Bescheinigung über die Eintragung,,

	• Nachweis, dass die Gesellschaft weiterhin besteht, • Eigentums-/Beteiligungsstruktur bis hin zum wirtschaftlichen Eigentümer, • Identitätsnachweis und Wohnanschrift der Person, die zur Unterzeichnung der erforderlichen Dokumente berechtigt ist, • Dokumente zur Überprüfung der Identität der Verwalter oder "gérants" der "société", • Letztes Register (oder gleichwertiges Dokument) mit den Namen, Adressen und Eigentumsanteilen der Mitglieder oder "associés", • Dokumente zur Überprüfung der Identität der Mitglieder oder "associés" der "société", • Dokumente zur Überprüfung der Identität des wirtschaftlichen Eigentümers, • Letzter Jahresabschluss oder Jahresbericht, falls vorhanden, und
Treuhandgesellschaft	• Treuhandvertrag oder einschlägige Auszüge mit Angabe der Namen des Treugebers, des Treuhänders, der Begünstigten, des Protektors, des Vollstreckers und des eigentlichen Rechts des Trusts, • Information des Treuhänders, dass der Trust weiterhin besteht, • Informationen über die Art und den Zweck des Trusts, • Angaben über die Herkunft des Treuhandvermögens, • Dokumente zur Überprüfung der Identität des Treugebers, des Treuhänders, der Begünstigten, des Protektors (falls vorhanden) und des Vollstreckers (falls vorhanden), • Identitätsnachweis und Wohnanschrift der Person, die berechtigt ist, die für den Erwerb erforderlichen Dokumente zu unterzeichnen • Angaben zum eingetragenen Sitz und zur Niederlassung des Treuhänders • Letzte Finanzübersicht des Trusts oder Jahresabschluss, falls vorhanden, und
Stiftung	• Satzung und/oder Statuten der Stiftung, • Falls die Stiftung eingetragen ist, Bescheinigung über die Eintragung, • Bestätigung des Stiftungsrats, dass die Stiftung weiterhin besteht, • Register oder gleichwertiges Dokument, aus dem die Namen und Anschriften der Mitglieder des Stiftungsrats, des Stifters und aller Personen, die der Stiftung Vermögen gestiftet haben, hervorgehen, • Angaben zum eingetragenen Sitz und zum

	Geschäftssitz der Stiftung, ● Dokumente zur Identitätsprüfung des Stifters, der Ratsmitglieder und der Begünstigten der Stiftung, ● Jüngste Finanzübersicht oder Finanzausweise, falls verfügbar, und

Wirtschaftliche Eigentümerschaft

Die Gesellschaft identifiziert und überprüft die Identität der wirtschaftlichen Eigentümer von juristischen Personen oder Vereinbarungen. In Übereinstimmung mit Vorschrift 6 der FIAML-Verordnungen 2018 erfolgt die Identifizierung der wirtschaftlichen Eigentümer durch die Anforderung von Informationen über:

1. die Identität aller natürlichen Personen, die letztlich eine Mehrheitsbeteiligung an der juristischen Person haben;
2. in Fällen, in denen gemäß Buchstabe a Zweifel bestehen, ob die Person mit der kontrollierenden Beteiligung der wirtschaftliche Eigentümer ist, oder in Fällen, in denen keine natürliche Person die Kontrolle über die Beteiligung ausübt, die Identität der natürlichen Person, die die Kontrolle über die juristische Person durch andere Mittel ausübt, die von der zuständigen Regulierungs- oder Aufsichtsbehörde festgelegt werden können; und
3. wenn keine natürliche Person gemäß Buchstabe a oder b identifiziert wird, die Identität der natürlichen Person, die die Position eines leitenden Angestellten innehat.

Die Identität der Person, die den Kunden letztlich besitzt oder kontrolliert (d.h. der wirtschaftliche Eigentümer), muss in jedem Fall festgestellt und überprüft werden.

7.1.3 Bevollmächtigte Personen oder Zeichnungsberechtigte

Einige Kunden (insbesondere juristische Personen) werden von Personen vertreten, die befugt sind, in ihrem Namen zu handeln.Das Unternehmen ist gesetzlich verpflichtet, die Identität und den aktuellen Wohnsitz jeder Person zu überprüfen, die behauptet, im Namen eines Kunden zu handeln. Das Unternehmen muss auch überprüfen, ob eine solche Person ordnungsgemäß bevollmächtigt ist, den Kunden zu vertreten oder in seinem Namen zu handeln. Daher müssen die in Tabelle 3 aufgeführten Informationen von jeder Person eingeholt werden, die behauptet, im Namen eines Kunden zu handeln.

Tabelle 3 - Von bevollmächtigten Personen anzufordernde Dokumente

Informationen	Quelle Dokument	Empfehlung
● Vollständiger Name (einschließlich früherer Namen) ● Datum und Ort der Geburt, ● Staatsangehörigkeit, ● Geschlecht ● Von der Regierung vergebene persönliche Identifikationsnummer oder andere von der Regierung	● Nationale Identitätskarte, oder ● Aktueller gültiger Reisepass, ● Ein offizielles Dokument, das die Namensänderung belegt (z. B. eine Heiratsurkunde, eine Bescheinigung über die Namensänderung), ● Das entsprechende staatliche Dokument, wie z. B. ein	Der Reisepass oder Personalausweis sollte mit einem Foto und der Unterschrift der Person versehen sein. Wenn der Kunde mehr als eine Staatsangehörigkeit hat, sollten Pässe oder nationale Ausweisdokumente für die zusätzliche Staatsangehörigkeit angefordert werden.

vergebene eindeutige Kennung	ausgestellter Gewerbeschein oder die Steuerkontonummer (TAN) der betreffenden Person.	
• Aktuelle und ständige Adresse	• eine Rechnung eines Versorgungsunternehmens (Festnetztelefonrechnung/Gasrechnung/Stromrechnung/Wasserrechnung), die innerhalb der letzten 3 Monate ausgestellt wurde, oder • ein Kontoauszug, der innerhalb der letzten 3 Monate ausgestellt wurde, oder • eine Kreditkartenabrechnung, die innerhalb der letzten 3 Monate ausgestellt wurde, oder • ein Schreiben einer professionellen Person, z. B. eines Rechtsanwalts, eines Wirtschaftsprüfers, eines Bankiers oder eines Notars, die die Person kennt. Das Schreiben sollte die ständige Wohnanschrift der Person enthalten.	Postfachadressen gelten nicht als ständige Wohnanschrift und können nicht akzeptiert werden. Rechnungen von Versorgungsunternehmen sollten auf den Namen des Kunden lauten. Wenn das Dokument auf den Namen eines Elternteils (Mutter oder Vater) lautet, sollte die Geburtsurkunde des Kunden vorgelegt werden. Ist die Rechnung auf den Namen eines Dritten ausgestellt, ist ein Schreiben des Dritten vorzulegen, in dem bestätigt wird, dass der Kunde an der auf der Rechnung angegebenen Adresse wohnt, und eine beglaubigte Kopie des Personalausweises des Dritten ist vorzulegen.
• Schriftlicher Nachweis, dass die Person befugt ist, im Namen des Kunden zu handeln	• Unterschriebener schriftlicher Beschluss, der die Person ermächtigt, den Kunden zu vertreten	Das Dokument muss den Namen der Person, ihre Beziehung zum Kunden, die zu erwerbende Immobilie, den Preis und die Tatsache enthalten, dass die Person befugt ist, den Kunden bei der Transaktion zu vertreten und alle für die Transaktion erforderlichen Dokumente zu unterzeichnen.

7.2 Originale oder beglaubigte Kopien von Dokumenten zur Identitätsüberprüfung

Wie bereits erwähnt, muss das Unternehmen die Identität seiner Kunden anhand zuverlässiger, unabhängiger Dokumente, Daten oder Informationen feststellen und überprüfen. Daher muss das Unternehmen sicherstellen, dass die Dokumente, auf die es sich bei der Identitätsüberprüfung stützt, korrekt sind und dass sie sich tatsächlich auf den Kunden beziehen.

In Fällen, in denen ein Angestellter oder ein leitender Angestellter des Unternehmens einen persönlichen Kontakt mit einem Kunden hatte und die Originaldokumente überprüft hat, kann dieser die Sorgfaltsprüfungsdokumente beglaubigen. Abgesehen

davon müssen die Prüfungsunterlagen des Kunden von einer geeigneten Person wie einem Rechtsanwalt, einem qualifizierten Buchhalter oder einer anderen professionellen Person beglaubigt werden. Eine fachkundige Person kann sein:

- ★ Notar,
- ★ ein Aktuar,
- ★ ein qualifizierter Buchhalter,
- ★ Angehörige der Justiz (Polizeibeamte, Richter, Staatsanwälte),
- ★ ein Mitarbeiter einer Botschaft oder eines Konsulats des Landes, dessen Staatsangehörigkeit die Person besitzt,
- ★ ein Manager, leitender Angestellter, Direktor oder Sekretär eines Finanzinstituts, das für AML-CFT-Zwecke reguliert wird.

Der Bescheiniger sollte angeben, dass die Kopie eine getreue Kopie des Originaldokuments ist. Der Bescheiniger muss die Kopie unterschreiben und mit seinem Stempel (falls vorhanden) versehen und seinen Namen, seine Anschrift und seine Berufsbezeichnung/Berufsbezeichnung sowie seine Kontaktdaten (d. h. eine Telefonnummer oder Adresse) deutlich angeben.

7.3 Screening

Im Rahmen der Identitätsprüfung müssen die Kunden und ihre Auftraggeber (wenn es sich bei den Kunden um juristische Personen oder Rechtsvereinbarungen handelt) überprüft werden. Das Screening erfolgt durch Abfragen unabhängiger und zuverlässiger Datenbanken auf der Grundlage der Informationen aus den erhaltenen Identitätsprüfungsdokumenten. Das Unternehmen verwendet für die Durchführung des Screenings, einschließlich des laufenden Screenings, eine geeignete Screening-Maschine.

Ziel des Screenings ist es, festzustellen, ob die Kunden (oder ihre Auftraggeber im Falle von Kunden, die juristische Personen oder Rechtsvereinbarungen sind):

- ★ politisch exponierte Personen sind; oder
- ★ Verbindungen zu organisiertem Verbrechen, Drogenhandel, Waffenhandel, Menschenhandel, Korruption ausländischer Beamter, Gewaltverbrechen oder Terrorismus haben; oder
- ★ wegen betrügerischer oder krimineller/anfechtbarer Handlungen verurteilt oder angeklagt sind oder waren.

Falls noch keine vollständigen Identitätsdokumente vorliegen, kann die Überprüfung auf der Grundlage der nachstehend aufgeführten Informationen durchgeführt werden, um den normalen Geschäftsablauf nicht zu stören. Sobald jedoch die Dokumente zur Identitätsüberprüfung vorliegen, sollten die Ergebnisse der Überprüfung mit den Dokumenten abgeglichen werden, um sicherzustellen, dass es keine Unstimmigkeiten gibt:

Für Einzelpersonen:

- ★ Name (einschließlich früherer Namen, anderer verwendeter Namen und sonstiger Aliasnamen)
- ★ Staatsangehörigkeit (einschließlich etwaiger weiterer Staatsangehörigkeiten)
- ★ Land des Wohnsitzes

Für juristische Personen oder Einrichtungen:

- ★ Name (einschließlich früherer Namen, anderer Geschäfts- oder Handelsnamen)
- ★ Land der Eintragung
- ★ Land, in dem das Unternehmen/die Tätigkeit ausgeübt wird

Die Ergebnisse der durchgeführten Überprüfung sollten als Teil der Identitätsprüfungsunterlagen des Kunden (in Papierform oder in Papierform) für die Dauer der Geschäftsbeziehung und für einen Zeitraum von mindestens sieben Jahren nach deren Beendigung aufbewahrt werden.

Wenn das Screening ergibt, dass der Kunde (oder einer seiner Auftraggeber):

- ★ eine politisch exponierte Person ist; oder
- ★ Verbindungen zu organisiertem Verbrechen, Drogenhandel, Waffenhandel, Menschenhandel, Korruption ausländischer Beamter, Gewaltverbrechen oder Terrorismus hat; oder
- ★ wegen betrügerischer oder krimineller/anfechtbarer Handlungen verurteilt oder beschuldigt worden ist,

Das Unternehmen muss die Geschäftsbeziehung als hochriskant behandeln und EDD-Maßnahmen anwenden, wie weiter unten in diesem Handbuch erläutert. Besteht der Verdacht, dass der Kunde versuchen könnte, die Produkte/Dienstleistungen des Unternehmens zu nutzen, um Geldwäsche und Terrorismusfinanzierung zu begehen, muss ein interner STR-Bericht (Vorlage siehe Anhang 3) an den MLRO geschickt werden, der dann prüft, ob ein STR-Bericht an die FIU geschickt werden muss.

Alle Screening-Berichte werden in den jeweiligen Kundenakten/Ordnern aufbewahrt.

7.4 Screening Engine

SumSub

Die Abteilung für Compliance und Risikomanagement wird das von Sumsub zur Verfügung gestellte Tool als Hauptunterstützungsinstrument verwenden. Sumsub speichert Informationen, die Finanzinstituten, Unternehmen, professionellen Dienstleistungsunternehmen, Regierungen, Strafverfolgungsbehörden, Aufsichtsbehörden und anderen Kunden und Unternehmen dabei helfen, Due-Diligence-Prüfungen und andere Screening-Aktivitäten in Übereinstimmung mit ihren rechtlichen oder regulatorischen Verpflichtungen und Risikomanagementverfahren im öffentlichen Interesse durchzuführen, einschließlich, aber nicht beschränkt auf die Zwecke der Bekämpfung von Geldwäsche oder "Kenne deinen Kunden", der Bekämpfung von Bestechung oder Korruption oder anderer Überprüfungen der Einhaltung von Vorschriften oder zur Verhinderung, Untersuchung, Aufdeckung oder Verfolgung von Finanzkriminalität, Betrug und schwerem Fehlverhalten oder Unehrlichkeit oder anderen kriminellen oder ungesetzlichen Aktivitäten (z. B. moderne Sklaverei, illegaler Handel, Umweltkriminalität usw.)) und jegliches unethische Verhalten.

Darüber hinaus bietet Sumsub Lösungen wie Benutzerüberprüfung, Transaktionsüberwachung, Geschäftsüberprüfung und Betrugsprävention.

Auf diese Weise können die Compliance-Beauftragten für jeden Kunden, Lieferanten, Geschäftspartner oder jede andere Gegenpartei schnell Überprüfungen in Bezug auf drei Hauptbereiche von Quellen durchführen:

1. Offizielle Quellen mit Schlüsselwörtern - Sanktionslisten, Durchsetzung von Vorschriften, Strafverfolgung
2. Medienquellen und unerwünschte Medien - Nachrichtenberichte, Zeitschriftenartikel, archivierte Nachrichtenaggregatoren, seriöse Medienquellen

3. Staatliche und offizielle Quellen - Gerichtsakten, Wahlergebnisse, Unternehmensanmeldungen, offizielle Unternehmenswebseiten und Pressemitteilungen.

Wie immer möchte sich das Unternehmen nicht ausschließlich auf automatische Tools verlassen, da es Erfahrungen mit möglichen Lücken oder maschinellen Missverständnissen gemacht hat, die ein Mensch (Compliance Officer) leicht verstehen könnte. Daher wird jeder Abgleich manuell von einem qualifizierten (und geschulten) Compliance-Beauftragten überprüft, um so volle Sicherheit über das Ergebnis zu erhalten.

Prüfung der Screening Engine

Um die Zuverlässigkeit und Integrität der Screening-Engine zu gewährleisten, führt das Unternehmen vor der Zeichnung eine Prüfung/Bewertung der Screening-Engine durch und bewahrt das Ergebnis der Prüfung/Bewertung in den Unterlagen auf. Dies ist ein wichtiger Schritt, wenn man bedenkt, dass das Unternehmen sich auf die Screening-Engine verlässt, um zu beurteilen, ob ein Kunde oder potenzieller Kunde ein PEP ist oder ob negative oder sanktionierende Informationen vorliegen, die seinem Profil entsprechen.

7.5 Überprüfung der Mittelherkunft

Die Tatsache, dass die Gelder für die Transaktion von einem Bankkonto oder einer Kredit-/Debitkarte überwiesen werden, entbindet das Unternehmen nicht von seiner Verpflichtung gemäß Abschnitt 3(2) des FIAMLA, die nach vernünftigem Ermessen erforderlichen Maßnahmen zu ergreifen, um sicherzustellen, dass weder das Unternehmen noch eine von ihm angebotene Dienstleistung von einer Person zur Begehung oder Erleichterung der Begehung eines Geldwäschedelikts oder der Terrorismusfinanzierung verwendet werden kann.

Als Mittelherkunft werden die Aktivitäten bezeichnet, die die Mittel für den Kauf des Grundstücks generiert haben:

- ★ Einkommen aus Beschäftigung
- ★ Einkommen aus unternehmerischer Tätigkeit
- ★ Darlehen
- ★ Verkauf von Immobilien
- ★ Verkauf von Investitionen
- ★ Schenkung
- ★ Erbschaft
- ★ Verkauf eines Unternehmens
- ★ Ausgleichszahlung
- ★ Erträge aus Investitionen/Sparen
- ★ Lotterie-/Glücksspielgewinn

Die Herkunft der Mittel kann durch eine Kombination von Quellen ermittelt werden, z. B. durch Angaben des Kunden, Informationen von Angehörigen reglementierter Berufe, die den Kunden kennen (Rechtsanwälte, Notare, Buchhalter, Banken), oder durch öffentlich zugängliche Informationen (Immobilienregister, Unternehmensregister, Medienberichte, Internetrecherchen usw.). Beispiele sind in der nachstehenden Tabelle aufgeführt:

Herkunft der Mittel zur Finanzierung der Transaktion	**Beispiele für Nachweise, die von Fall zu Fall anwendbar sein können**
Einkommen aus Beschäftigung	● Lebenslauf mit Angaben zu den Unternehmen und den bekleideten Positionen oder ● Einkommensangaben des Arbeitgebers, oder ● Jüngste Abrechnungen bei Selbstständigen, oder ● Kontoauszüge, aus denen der Eingang der letzten drei Monate regelmäßiger Gehaltszahlungen des genannten Arbeitgebers hervorgeht, oder ● Steuererklärung.
Einkommen aus unternehmerischer Tätigkeit	● Finanzausweise oder Konten, ● Bankauszüge des betreffenden Unternehmens. ● Unabhängige Informationen aus öffentlichen Quellen, die die Informationen bestätigen
Darlehen	● Darlehensvertrag
Verkauf von Immobilien	● Kaufvertrag, oder ● Bankauszug, aus dem die Verkaufssumme hervorgeht, oder ● Schreiben eines Buchhalters oder eines Notars, das den Verkauf bestätigt, oder ● Medienberichterstattung (falls zutreffend) über den Verkauf.
Verkauf von Investitionen	● Urkunden, Schlussnoten oder Erklärungen im Namen des Kunden, die den Verkauf belegen.
Schenkung	● Rechtsdokumente zum Nachweis der Schenkung, sofern möglich; oder ● Schriftliche Erklärung des Schenkers zur Bestätigung der Schenkung.
Erbschaft	● Rechtsdokument mit vollständigen Angaben zum geerbten Vermögen; oder ● Bankauszug, wenn er den vollständigen Namen und die Adresse des Kunden enthält und die Herkunft der Gelder deutlich macht.
Verkauf eines Unternehmens	● Kaufvertrag, oder ● Rechtsdokument, das den Verkauf belegt, oder ● Medienberichterstattung (falls zutreffend) über den Verkauf, oder ● Unterzeichnetes Schreiben eines Buchhalters oder Notars, das den Verkauf bestätigt.
Ausgleichszahlung	● Schreiben der entschädigenden Stelle; oder

	• Gerichtsdokumente, in denen die Einzelheiten des Anspruchs dargelegt sind; oder • Rechtsdokument, das die Entschädigungszahlung belegt.
Erträge aus Investitionen/Sparen	• Zertifikate, Schlussnoten oder Auszüge auf den Namen des Antragstellers; oder • eine Bestätigung der betreffenden Investmentgesellschaft; oder • Kontoauszug, aus dem hervorgeht, dass das Geld von der Investmentgesellschaft eingegangen ist.
Lotterie-/Glücksspielgewinn	• Schreiben der zuständigen Organisation (Lotterie • Zentrale/Wettbüro/Kasino), oder • Kontoauszug, aus dem hervorgeht, dass das Geld von der betreffenden Organisation eingezahlt wurde, oder • Medienberichterstattung (falls zutreffend) über den Gewinn.

Alle Informationen, die im Zusammenhang mit der Überprüfung der Herkunft der Mittel eines Kunden eingeholt werden, müssen in geeigneter Weise aufgezeichnet werden. Die vom Kunden gestellten Fragen und gegebenen Antworten sowie die zur objektiven Überprüfung der Informationen getroffenen Maßnahmen müssen dokumentiert werden. Die Aufzeichnungen sollten es einem unabhängigen Prüfer, z. B. einem Untersuchungsbeauftragten, ermöglichen, nachzuvollziehen, wie das Unternehmen die Herkunft der Gelder des Kunden festgestellt hat.

Mindestbetrag für die Kontoeröffnung

Die Mindesteinlage, die für die Kontoeröffnung akzeptiert wird, beträgt 50 $.

In Bezug auf andere Kundenkategorien, einschließlich, aber nicht beschränkt auf Geldverwalter, Finanzberater, institutionelle und große Geldverwalter und ähnliche Unternehmen, führt das Unternehmen eine vollständige Due-Diligence-Prüfung in Übereinstimmung mit dem oben beschriebenen Verfahren der Sorgfaltspflicht gegenüber Kunden durch und prüft, ob sie aus Sicht der AML/CFT ordnungsgemäß von einer Aufsichtsbehörde/Behörde in einem Land reguliert werden, das mindestens gleichwertige AML/CFT-Gesetze wie Mauritius hat. In Fällen, in denen diese Unternehmen die Plattform nutzen möchten, um Kundenportfolios individuell zu verwalten (d. h., es werden Konten im Namen der Kunden eröffnet), stellt das Unternehmen außerdem sicher, dass alle diese Kunden ordnungsgemäß identifiziert werden und ihre Identität gemäß dem in diesem Handbuch dargelegten Verfahren der Sorgfaltspflicht gegenüber Kunden überprüft wird, einschließlich der Überprüfung der Herkunft der Mittel.

7.6 AML-CFT-Risikobewertung der Kunden

In Übereinstimmung mit Abschnitt 17(1) FIAMLA wird auf der Grundlage der gesammelten Identifikationsdokumente und des Ergebnisses der Überprüfung eine AML-CFT-Risikobewertung des Kunden durchgeführt. Zu diesem Zweck wird eine

Risikobewertung des Kunden unter Verwendung des Customer Risk Assessment Tool durchgeführt, um das Ausmaß der ML/TF-Risiken zu bestimmen, die mit der Geschäftsbeziehung zu dem Kunden verbunden sind.

7.6.1 Hochrisikokunden und verstärkte Sorgfaltspflichtmaßnahmen

Wird ein Kunde als hochriskant eingestuft, z. B. wenn der Kunde oder sein wirtschaftlicher Eigentümer oder einer seiner Auftraggeber ein PEP ist, ist das Unternehmen gemäß den Verordnungen 12 und 15 der FIAMLR verpflichtet, Maßnahmen zur verstärkten Sorgfaltspflicht anzuwenden. Eine verstärkte Sorgfaltspflicht (EDD) bedeutet, dass zusätzliche Schritte im Vergleich zur regulären Identitätsüberprüfung, die im Allgemeinen durchgeführt wird, unternommen werden. Wie in den vorgenannten Verordnungen festgelegt, umfassen EDD-Maßnahmen Folgendes

1. Einholung zusätzlicher Informationen über den Kunden (z. B. Beruf, Umfang des Vermögens, Informationen aus öffentlichen Datenbanken, Internet usw.) und regelmäßigere Aktualisierung der Identifikationsdaten des Kunden und des wirtschaftlichen Eigentümers;
2. Einholung zusätzlicher Informationen über den beabsichtigten Charakter der Geschäftsbeziehung;
3. Einholung von Informationen über die Herkunft der Mittel und des Vermögens des Kunden;
4. Einholung von Informationen über die Gründe für beabsichtigte oder durchgeführte Transaktionen;
5. Einholung der Genehmigung der Geschäftsleitung für die Aufnahme oder Fortsetzung der Geschäftsbeziehung;
6. eine verstärkte Überwachung der Geschäftsbeziehung, indem die Anzahl und der Zeitpunkt der durchgeführten Kontrollen erhöht und Transaktionsmuster ausgewählt werden, die einer weiteren Prüfung bedürfen;

Für Hochrisikokunden muss die Genehmigung der Geschäftsleitung eingeholt werden, ob die Geschäftsbeziehung aufgenommen (wenn es sich um einen neuen Kunden handelt), fortgesetzt (wenn es sich um einen bestehenden Kunden handelt) oder beendet werden soll (siehe Vorlage in Anhang 1). Zu diesem Zweck müssen vollständige Informationen über die Verfügbarkeit von Dokumenten zur Identitätsprüfung, die Ergebnisse des Screenings und die verfügbaren EDD-Dokumente vorgelegt werden, um eine fundierte Entscheidung zu ermöglichen.

7.6.2 EDD für Einzelpersonen

Handelt es sich bei dem Kunden um eine Einzelperson, die im eigenen Namen handelt und als Hochrisikokunde eingestuft wird, z. B. weil es sich um einen PEP, ein Familienmitglied oder einen engen Mitarbeiter eines PEP handelt, holt das Unternehmen im Rahmen der EDD-Maßnahme weitere Informationen über die Herkunft des Vermögens und andere Informationen/Dokumente ein, einschließlich, aber nicht beschränkt auf die Einholung einer Bankreferenz, die innerhalb der letzten drei Monate ausgestellt wurde. Solange die Geschäftsbeziehung mit dem Kunden andauert, stellt das Unternehmen außerdem im Rahmen einer EDD-Maßnahme sicher, dass die Dokumente zur Identitätsprüfung des Kunden aktuell und gültig sind. So darf beispielsweise die Kopie des Reisepasses in den Unterlagen nicht abgelaufen sein, und der Adressnachweis in den Unterlagen muss korrekt sein (d. h. Adresse und Name des Kunden haben sich in der Zwischenzeit nicht geändert). Das Unternehmen führt außerdem verstärkte Recherchen und Analysen der Hochrisikofaktoren durch, die in den Akten dokumentiert werden, um die Risiken weiter zu mindern. Beachten Sie, dass die vorgenannten Maßnahmen nicht erschöpfend sind und hauptsächlich von der Art des Risikos abhängen, das der Kunde bzw. potenzielle Kunde darstellt.

Quelle des Vermögens und Quelle der Mittel sind zwei unterschiedliche Dinge. Die Quelle des Vermögens ist definiert als die Tätigkeit oder das Ereignis, durch die bzw. das das Nettovermögen der Person entstanden ist (und nicht nur die Mittel, die für die

vorliegende Transaktion verwendet werden). Die Herkunft des Vermögens kann auch durch eine Kombination von Quellen überprüft werden, z. B. durch Informationen, die der Kunde zur Verfügung stellt, Bestätigungen von regulierten Fachleuten, die den Kunden kennen (Rechtsanwälte, Notare, Buchhalter, Banken) oder öffentlich zugängliche Informationen (Immobilienregister, Unternehmensregister, Medienberichte, Internetrecherchen usw.).

Ein Bankreferenzschreiben belegt, dass (i) die Identität und Adresse des Kunden von einer unabhängigen Institution überprüft wurde und (ii) dass der Kunde auch Kunde eines Finanzinstituts ist, das für AML-CFT reguliert wird.

Die Bankreferenz sollte auf dem Briefkopf der Bank ausgestellt werden und eindeutig das Datum, an dem das Schreiben ausgestellt wurde, den Namen und Titel des Bankangestellten sowie die Kontaktdaten der Bank enthalten. Das Bankreferenzschreiben sollte den Zeitraum angeben, in dem die Person Kunde der Bank war, und bestätigen, dass die Bankbeziehung akzeptabel war, ohne dass die Person ein Versäumnis begangen hat. Darüber hinaus führt das Unternehmen erweiterte Recherchen durch und dokumentiert die Ergebnisse, die bei der Person erzielt wurden.

Die EDD-Maßnahmen hängen von der Art des Risikos ab, und es gibt daher keine maßgeschneiderte Liste von Dokumenten, die in der Regel erforderlich wären.

7.6.3 EDD zur juristischen Person oder Rechtsvereinbarung

Handelt es sich bei dem Kunden um eine juristische Person oder Rechtsvereinbarung, hängt die EDD-Maßnahme von dem Grund ab, aus dem die juristische Person oder Rechtsvereinbarung als Hochrisiko eingestuft wurde. Zum Beispiel:

- ★ Handelt es sich bei dem Kunden um eine juristische Person, die aufgrund des Ergebnisses des Screenings ihres Anteilseigners (oder einer gleichwertigen Funktion in der juristischen Person oder Vereinbarung) oder ihres wirtschaftlichen Eigentümers als hohes Risiko eingestuft wird, so wird die EDD angewandt, indem die Quelle des Vermögens des betreffenden Anteilseigners oder wirtschaftlichen Eigentümers ermittelt und dokumentiert wird und alle anderen Informationen, die vernünftigerweise erforderlich sind, um das Risiko zu dokumentieren und zu mindern;

- ★ Wird der Kunde aufgrund des Ergebnisses der Überprüfung seines Geschäftsführers (oder einer gleichwertigen Funktion in der juristischen Person oder Vereinbarung) als hohes Risiko eingestuft, so wird die EDD angewandt, indem sichergestellt wird, dass (i) keine Gelder oder Vermögenswerte des betreffenden Geschäftsführers in eine Transaktion mit der Gesellschaft involviert sind und dass (ii) der betreffende Geschäftsführer nicht der wirtschaftliche Eigentümer der juristischen Person ist. Die Art des hohen Risikos, das von dem Geschäftsführer ausgeht, wird durch weitere Recherchen überprüft;

- ★ In Fällen, in denen der Kunde aufgrund negativer Informationen über den Kunden selbst als hohes Risiko eingestuft wird, wird die EDD angewandt, indem weitere Informationen eingeholt werden, um den rechtmäßigen Zweck der Transaktion mit der Gesellschaft zu ermitteln. Das Unternehmen ergreift auch alle angemessenen Maßnahmen, um sicherzustellen, dass seine Dienstleistungen nicht für illegale Zwecke genutzt werden, falls es beschließt, eine Geschäftsbeziehung mit dem Kunden einzugehen.

Bei der Aufnahme neuer Kunden müssen die EDD-Dokumente vor der Aufnahme der Geschäftsbeziehung mit dem Kunden eingeholt werden. Vor allem müssen EDD-Dokumente und/oder Informationen eingeholt werden, bevor eine Einzahlung oder Überweisung von Geldern des Kunden akzeptiert wird. Wenn der Kunde bereits an Bord ist, müssen die EDD-Dokumente eingeholt werden, bevor die Transaktion fortgesetzt wird.

Alle Informationen, die sich auf den EDD eines Kunden beziehen, müssen in angemessener Weise aufgezeichnet werden. Die Aufzeichnungen sollten ausreichen, um einem unabhängigen Prüfer, z. B. einem Ermittler der FIU oder einer zuständigen Behörde, nachzuweisen, wie das Unternehmen die EDD beim Kunden durchgeführt hat, um sicherzustellen, dass seine Dienstleistungen nicht für unrechtmäßige Zwecke genutzt werden.

7.6.4 Politisch exponierte Personen (PEP)

Politisch exponierte Personen sind Personen, die mit herausragenden öffentlichen Funktionen/Positionen betraut sind oder waren (z. B. Staats- oder Regierungschefs, hochrangige Politiker, hochrangige Regierungs-, Justiz- und Militärbeamte, leitende Angestellte staatlicher Unternehmen und wichtige Parteifunktionäre) sowie deren Verwandte und Mitarbeiter.

Dazu gehören:

1. Personen, die die Definition eines PEP in Mauritius erfüllen (d. h. ein inländischer PEP),
2. Personen, die die Definition eines PEP in einem anderen Land erfüllen (d.h. ausländische PEP) und
3. Personen, die von einer internationalen Organisation mit einer herausgehobenen Funktion/Position betraut wurden, einschließlich Mitgliedern der Geschäftsleitung oder anderen Funktionen, die Direktoren, stellvertretenden Direktoren und Vorstandsmitgliedern entsprechen (d.h. PEP einer internationalen Organisation).

Die Definition von PEPs würde auch Familienmitglieder und enge Mitarbeiter von PEPs einschließen. Nahe stehende Personen und Familienmitglieder werden im Folgenden definiert:

“close associates” —

1. eine Person, die mit einem PEP entweder gesellschaftlich oder beruflich eng verbunden ist; und
2. schließt jede andere Person ein, die von einer Aufsichtsbehörde oder Regulierungsstelle nach Rücksprache mit dem Nationalen Ausschuss festgelegt werden kann;

"Familienmitglieder" -

1. eine Person, die mit einer PEP entweder direkt durch Blutsverwandtschaft oder durch Heirat oder ähnliche Formen der Lebenspartnerschaft verwandt ist; und
2. schließt jede andere Person ein, die von einer Aufsichtsbehörde oder Regulierungsstelle nach Rücksprache mit dem Nationalen Ausschuss festgelegt werden kann.

PEPs stellen unter dem Gesichtspunkt der Geldwäsche und der Terrorismusfinanzierung ein höheres Risiko dar, da sie eher geneigt sind, von Korruptionserlösen zu profitieren, und auch, weil sie (aufgrund ihrer Ämter und Verbindungen) potenziell die Erlöse aus Korruption oder anderen Straftaten verbergen können.

Wenn ein Kunde oder wirtschaftlicher Eigentümer (entweder durch ein Screening oder durch verfügbare Informationen) als PEP identifiziert wurde, muss zusätzlich zu den oben genannten EDD-Maßnahmen eine spezielle Genehmigung der Geschäftsleitung

eingeholt werden, bevor die Geschäftsbeziehung aufgenommen oder fortgesetzt wird; hierzu ist das als Anhang 1 beigefügte Formular zu verwenden.

Wenn ein Kunde oder ein Auftraggeber eines Kunden (im Falle einer juristischen Person oder einer Vereinbarung) als PEP identifiziert wird (durch Überprüfung der eingegangenen CDD-Maßnahmen, während des Screening-Prozesses usw.), ist außerdem das PEP-Protokoll (Anhang 10) entsprechend auszufüllen.

7.6.5 Verbotene Kunden

Mit einem Kunden, der nach der Kundenrisikobewertung als verboten eingestuft wurde, sollte keine Geschäftsbeziehung aufgenommen werden. Das Unternehmen stellt die Geschäftsbeziehungen mit dem Kunden unverzüglich ein, und bei Bedarf wird ein Bericht über verdächtige Transaktionen bei der FIU eingereicht. Eine Liste der verbotenen Kunden ist unten aufgeführt:

1. Liste der verbotenen Kunden (gilt sowohl für natürliche als auch für juristische Personen oder Rechtsvereinbarungen)
    a. Personen, die im Rahmen des Screening-Prozesses auf Sanktionslisten (z. B. Sanktionsliste der Vereinten Nationen oder vom Nationalen Sanktionsausschuss erstellte Liste) aufgeführt sind;
    b. Personen, deren Vermögenswerte gemäß dem Gesetz über gefährliche Drogen eingefroren wurden;
    c. Personen, die wegen Geldwäsche und/oder Terrorismusfinanzierung in Mauritius oder im Ausland verurteilt worden sind;
    d. Personen, gegen die derzeit von einer lokalen oder ausländischen Behörde wegen Geldwäsche, Terrorismusfinanzierung, Korruption, Bestechung, Betrug oder anderen Finanzdelikten ermittelt wird.

7.6 Zeitplan für die Identitätsprüfung, das Screening und die Risikobewertung der Kunden

In der Onboarding-Phase müssen vom Kunden Dokumente zur Identitätsprüfung angefordert werden. Es müssen alle angemessenen Maßnahmen ergriffen werden, um alle erforderlichen Dokumente zur Identitätsüberprüfung zu erhalten, ein Screening durchzuführen und eine Risikobewertung des Kunden vor der Aufnahme der Kundenbeziehung und der Kontoeröffnung vorzunehmen.

7.6.1 Wenn keine Dokumente zur Identitätsüberprüfung oder EDD-Dokumente beschafft werden können

Gemäß Regulation 13 der FIAML Regulations 2018 darf keine Geschäftsbeziehung hergestellt/keine Transaktion durchgeführt/keine Beziehung beendet werden und es muss eine STR bei der FIU eingereicht werden, wenn das Unternehmen nicht alle erforderlichen Informationen zur Feststellung der Identität des Kunden erhalten kann.

Gemäß Regulation 12(3) der FIAML Regulations 2018 ist das Unternehmen verpflichtet, die Geschäftsbeziehung zu beenden und einen STR bei der FIU einzureichen, wenn es nicht in der Lage ist, die erforderlichen EDD-Maßnahmen durchzuführen. Daher ist ein interner STR an die MLRO zu übermitteln, wenn

1. Identitätsprüfungsdokumente können nicht zu seiner Zufriedenheit über den Kunden und einen seiner Auftraggeber eingeholt werden (falls der Kunde eine juristische Person/Rechtsvereinbarung ist), und/oder

2. EDD-Maßnahmen müssen angewendet werden, aber die erforderlichen EDD-Dokumente/Informationen können vom Kunden nicht beschafft werden.

8. Kundenakzeptanz

Risikobasierter Ansatz

Um zu vermeiden, dass die Regelungen einer Firma zu einer restriktiven oder schwerfälligen Belastung werden, muss sie sicherstellen, dass ihr eingebetteter Ansatz und ihre Kontrollen die Kernelemente eines risikobasierten Ansatzes in dieser Hinsicht befolgen und widerspiegeln. Dazu gehört insbesondere, dass man sich vergewissern muss, dass man (sowohl rechtlich als auch wirtschaftlich) weiß, wer der oder die Kunden tatsächlich sind, und dass man die Art und den Zweck bzw. die Erwartungen kennt, mit denen ein Kunde eine Geschäftsbeziehung anstrebt. Von den beaufsichtigten Firmen wird jedoch auch erwartet, dass sie geeignete Maßnahmen und unabhängige Quellen und Unterlagen anwenden und nutzen, um Kunden zu identifizieren und diese Identität gesondert zu überprüfen, während sie gleichzeitig eine relevante risikobasierte Sorgfaltsprüfung (CDD) für ihre Kunden auf einer anfänglichen und laufenden Basis durchführen. Für das Unternehmen könnte sich dies auf die Anwendung von Ermittlungs- und Kontrollmaßnahmen erstrecken, um die zugrundeliegende und rechtmäßige Geldquelle (Source of Funds, SoF) und/oder die Herkunft des Vermögens zu ermitteln und zu überprüfen, d. h. wie und woher die Anlagegelder stammen, die für Kontoeinlagen und Transaktionen verwendet werden, z. B. realistisches Einkommen, eine Erbschaft oder frühere Investitionen/Ersparnisse usw. Es kann jedoch auch bedeuten, dass die Firmen flexibel und pragmatisch sein müssen, welche Unterlagen verlangt und akzeptiert werden, um ihre aufsichtsrechtlichen und gesetzlichen Pflichten zu erfüllen und ein reibungsloses Funktionieren der Kundenbeziehungen zu ermöglichen.

Die wichtigsten Bestandteile der KYC sind:

- ★ Identitätsüberprüfung: Um ein neues Konto zu eröffnen, müssen Personen einen gültigen amtlichen Ausweis vorlegen, z. B. einen Reisepass, einen Führerschein oder einen Personalausweis, um ihre Identität zu bestätigen.
- ★ Überprüfung der Adresse: Um den Wohnsitz des Kunden zu bestätigen, ist ein Adressnachweis erforderlich, z. B. Rechnungen von Versorgungsunternehmen oder Kontoauszüge.
- ★ Sorgfältige Prüfung des Kunden: Das Unternehmen muss seine Kunden einer Sorgfaltsprüfung unterziehen. Dazu gehört unter anderem die Bewertung des Risikoprofils des Kunden, seiner geschäftlichen Aktivitäten, der wirtschaftlichen Eigentümer und der Herkunft der Mittel.
- ★ Laufende Überwachung: KYC ist kein einmaliger Vorgang. Das Unternehmen ist verpflichtet, die Kundendateien (entsprechend der zugewiesenen Risikoeinstufung) kontinuierlich zu überwachen, um verdächtige Aktivitäten zu erkennen und zu melden.

Elektronische Identifizierung und Überprüfung

Führt das Unternehmen ein System zur elektronischen Überprüfung der Identität einer natürlichen Person ein, muss es die Zuverlässigkeit der dem System innewohnenden Kontrollen bewerten, um festzustellen, ob es sich auf die erzielten Ergebnisse verlassen kann oder ob zusätzliche Schritte zur Ergänzung der bestehenden Kontrollen erforderlich sind. Zu den von der Gesellschaft unternommenen zusätzlichen Schritten könnte gehören, dass ein Vertreter der Gesellschaft oder ein benannter Dritter, z. B. ein Rechtsanwalt, ein Notar oder ein Buchhalter, bei der Verwendung der Onboarding-Software mit der natürlichen Person anwesend sein muss.

Unter allen Umständen wird das Unternehmen einen risikobasierten Ansatz verfolgen, um sich zu vergewissern, dass die erhaltenen Dokumente ausreichend belegen, dass der Kunde derjenige ist, der er vorgibt zu sein, und dass das Unternehmen von der Echtheit dieser Dokumente überzeugt ist. Das Unternehmen prüft die Art der Datei und stellt sicher, dass sie fälschungssicher ist, es könnte die E-Mail-Adresse prüfen, von der sie empfangen wird, um sicherzustellen, dass sie legitim erscheint und sich auf

den Kunden bezieht, der die Unterlagen einreicht, wenn das Dokument zertifiziert wurde, dass es sich um einen geeigneten Zertifizierer handelt usw.

Wenn das Unternehmen aufgrund der elektronischen Erfassung nicht sicher ist, ob die Dokumente echt sind oder ob sie sich tatsächlich auf den Kunden beziehen, sollte ein kumulativer Ansatz verfolgt und zusätzliche Maßnahmen oder Überprüfungen durchgeführt werden, um sich Gewissheit zu verschaffen. Wenn die Überprüfung der Identität oder der Adresse immer noch nicht zufriedenstellend ist, darf die Geschäftsbeziehung nicht fortgesetzt werden, das Unternehmen wird die Geschäftsbeziehung beenden und eine interne Offenlegung in Betracht ziehen.

8.1 Onboarding-Prozess für Kunden

8.1.1 Anforderung von Dokumenten zur Identitätsprüfung

Vorgeschlagene Kunden, die sich auf der Website des Unternehmens registrieren lassen, um die Dienstleistungen des Unternehmens in Anspruch zu nehmen, müssen während der Registrierungsphase relevante Informationen zur Verfügung stellen und die geforderten Nachweisdokumente vorlegen.

8.1.2 Screening durchführen

Sobald sich der vorgeschlagene Kunde auf der Website des Unternehmens registriert und die relevanten Informationen und Dokumente eingereicht hat, erhält das Onboarding-Team diese Informationen und Dokumente und fährt mit der Prüfung fort.

8.1.3 Kundenrisikobewertung durchführen

Nach Abschluss des Screenings führt die Compliance-Abteilung (der zuständige Beamte) die Risikobewertung des Kunden mit Hilfe des zu diesem Zweck entwickelten Kundenrisikobewertungs-Tools durch. Die Dokumente zur Identitätsüberprüfung und die Screening-Berichte müssen bei der Durchführung der Bewertung berücksichtigt werden. Handelt es sich um einen Kunden mit hohem Risiko, sind entsprechende EDD-Maßnahmen zu ergreifen.

Sobald die oben genannten Schritte abgeschlossen sind, wird der Kunde akzeptiert und die Dokumente werden in das CRM des Unternehmens hochgeladen.

Kunden mit hohem Risiko

Für Kunden mit hohem Risiko und Geschäftsbeziehungen, an denen PEPs beteiligt sind, muss, wie bereits erwähnt, die Genehmigung der Geschäftsleitung eingeholt werden. Zu diesem Zweck hat er die Risikobewertung des Kunden zu berücksichtigen und:-

1. die Dokumente zur Identitätsüberprüfung, das Ergebnis des Screenings, die Risikobewertung des Kunden und die EDD-Dokumente des Kunden zu bewerten,
2. die vorgeschlagenen Dienstleistungen für den Kunden in Betracht ziehen und
3. eine Entscheidung über das weitere Vorgehen durch Unterzeichnung des Dokuments in Anhang 1 zu treffen.

9. Einzahlungskanal

In Anbetracht des Risikos der Geldwäsche und der Terrorismusfinanzierung nimmt die Gesellschaft Einzahlungen von Kunden nur durch direkte Überweisung von einem Bankkonto, das auf den Namen des Kunden lautet, oder durch Kreditkarten/Debitkarten/Prepaidkarten/regionale Zahlungslösungen auf den Namen des Kunden an. Die Gesellschaft nimmt keine Einlagen von Dritten an. Darüber hinaus akzeptiert die Gesellschaft auch Einzahlungen über Skrill und Neteller.

Einzahlungen werden über geeignete Zahlungsdienstleister ("PSP") abgewickelt, die Zahlungsgateway-Dienste anbieten. In der Praxis werden die Gelder dem Konto des Zahlungsdienstleisters gutgeschrieben, der nach Abzug der vereinbarten Transaktionsgebühren die Gelder auf das Kundenkonto des Unternehmens einzahlt, damit die Handelsaktivitäten stattfinden können.

Der zulässige Mindestbetrag für Einzahlungen beträgt 50 USD und der zulässige Höchstbetrag pro Einzahlung 5.000 USD (dies ist ein tägliches Limit für Einzahlungen).

10. Kontinuierliche Überwachung

Gemäß Verordnung 3 (1) (e) ist das Unternehmen rechtlich verpflichtet, eine laufende Überwachung einer Geschäftsbeziehung durchzuführen, bis die Geschäftsbeziehung mit einem Kunden beendet ist. Die laufende Überwachung erfolgt nach einem risikobasierten Ansatz, um eine angemessene Zuweisung von Ressourcen zu gewährleisten.

10.1 Laufende CDD-Überwachung

Die laufende CDD-Überwachung wird wie nachstehend beschrieben durchgeführt:

10.1.1 Für Hochrisikokunden - Mindestens jährlich

Der laufende Überwachungsprozess wird jährlich ab dem Datum der letzten Risikobewertung des Kunden durchgeführt.

Für Hochrisikokunden:

- ★ Aktuelle Ausweisdokumente, die vom Kunden angefordert werden müssen, und erneute Überprüfung vor der Durchführung einer weiteren Transaktion (einschließlich der Annahme einer weiteren Einzahlung)
- ★ Aktualisierung der Kundeninformationen wie Beruf und andere relevante Informationen
- ★ Erneute Risikobewertung des Kunden, um die vom Kunden ausgehenden Risiken neu zu bewerten
- ★ Ausfüllen des Formulars "Laufende Überwachung" (Anhang 2)
- ★ Abhängig von verschiedenen Aspekten (z. B. von den Transaktionsmustern/Aktivitäten) können weitere Dokumente vom Kunden verlangt werden
- ★ Bewertung der Hochrisikofaktoren und verstärkte Recherchen/Analysen derselben

Die fortlaufende CDD-Überwachung wird danach jährlich durchgeführt.

10.1.2 Für Kunden mit mittlerem Risiko - alle 2 Jahre

Der laufende Überwachungsprozess wird alle 2 Jahre ab dem Datum der letzten Risikobewertung des Kunden durchgeführt.

Für Kunden mit mittlerem Risiko:

- ★ Anforderung aktueller Ausweisdokumente vom Kunden und erneute Überprüfung vor der Durchführung einer weiteren Transaktion (einschließlich der Annahme einer weiteren Einzahlung)
- ★ Erneute Risikobewertung des Kunden, um die vom Kunden ausgehenden Risiken neu zu bewerten
- ★ Aktualisierung der Kundeninformationen wie Beruf und andere relevante Informationen
- ★ Ausfüllen des Formulars "Laufende Überwachung" (Anhang 2)
- ★ Abhängig von verschiedenen Aspekten (z. B. von den Transaktionsmustern/Aktivitäten) können weitere Dokumente vom Kunden verlangt werden

Die fortlaufende Überwachung wird danach alle 2 Jahre durchgeführt.

10.1.3 Für Kunden mit geringem Risiko - Alle 3 Jahre

Der laufende Überwachungsprozess wird alle 3 Jahre ab dem Datum der letzten Risikobewertung des Kunden durchgeführt.

Für Low-Risk-Kunden:

- ★ Anforderung aktueller Ausweisdokumente vom Kunden und erneute Überprüfung vor der Durchführung einer weiteren Transaktion (einschließlich der Annahme einer weiteren Einzahlung)
- ★ Erneute Risikobewertung des Kunden, um die vom Kunden ausgehenden Risiken neu zu bewerten
- ★ Ausfüllen des Formulars "Laufende Überwachung" (Anhang 2)
- ★ Aktualisierung der Kundeninformationen wie Beruf und andere relevante Informationen
- ★ Abhängig von verschiedenen Aspekten (z. B. von den Transaktionsmustern/Aktivitäten) können weitere Dokumente vom Kunden verlangt werden

Die fortlaufende CDD-Überwachung wird danach jedes Jahr durchgeführt.

10.1.4 Laufende CDD-Überwachung Tabelle

Risikobewertung	**Häufigkeit der fortlaufenden Überwachung**
Gering	Alle 3 Jahre
Mittel	Alle 2 Jahre
Hoch	Jährlich

10.2 Überwachung von Vorgängen

Die Transaktionsüberwachung ist ein wesentlicher Bestandteil des Rahmens für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung, da sie die unverzügliche Ermittlung verdächtiger Transaktionen ermöglicht. Das Transaktionsmonitoring wird wie unten beschrieben durchgeführt:

1. Überwachung der Einlagen
   Die Gesellschaft überwacht die von den Kunden für den künftigen Handel getätigten Einlagen. Das Unternehmen muss insbesondere Folgendes berücksichtigen:
   a. ob der eingezahlte Betrag dem Kundenprofil angemessen ist
   b. ob das Muster/die Häufigkeit der Einzahlungen dem Kundenprofil und den erwarteten Einzahlungen angemessen ist
   c. ob die Einzahlungen direkt von einem Bankkonto oder einer Kredit-/Debit-/Prepaid-Karte im Namen des Kunden vorgenommen werden

2. Überwachung des Gewerbes
   Das Unternehmen stellt eine angemessene Überwachung der Handelsaktivitäten der Kunden auf der Handelsplattform sicher. Insbesondere hat das Unternehmen Folgendes zu beachten:
   a. ob das Handelsmuster keine rechtmäßigen oder wirtschaftlichen Ziele zu verfolgen scheint
   b. ob das Handelsmuster nicht dem Kundenprofil und den Anlagezielen zu entsprechen scheint

3. Überwachung der Rücknahme/Rücknahme
   Die Gesellschaft sorgt für eine angemessene Überwachung der von den Kunden beantragten Rücknahmen/Rückkäufe. Insbesondere muss das Unternehmen Folgendes berücksichtigen:
   a. ob die Gesamtaktivität des Kunden bis zur Abhebung wirtschaftlich sinnvoll ist
   b. ob die zur Abhebung beantragten Gelder auf ein Bankkonto oder eine Kreditkarte überwiesen werden, die auf den Namen des Kunden registriert sind
   c. ob das Abhebungsverhalten dem Kundenprofil und dem Anlageziel angemessen ist

Das Screening muss durch Abfragen unabhängiger und zuverlässiger Datenbanken unter Verwendung der erhaltenen Dokumente zur Identitätsüberprüfung erfolgen, um sicherzustellen, dass in der Zwischenzeit (d. h. vom Zeitpunkt des ersten Screenings bis zur Zahlung der endgültigen Kaution) der Kunde oder einer seiner Auftraggeber (falls der Kunde eine juristische Person ist) nicht als solcher gemeldet wurde:

- ★ ein PEP, ein Familienmitglied oder ein enger Vertrauter eines PEP ist; oder
- ★ keine Verbindungen zu organisiertem Verbrechen, Drogenhandel, Waffenhandel, Menschenhandel, Korruption ausländischer Beamter, Gewaltverbrechen oder Terrorismus hat; oder
- ★ keine Verurteilungen oder Anschuldigungen wegen betrügerischer oder krimineller/zweifelhafter Aktivitäten vorliegen oder vorgelegen haben.

Wenn die Ergebnisse des Screenings unwiderlegbar zeigen, dass der Kunde oder einer seiner Auftraggeber (falls es sich bei dem Kunden um eine juristische Person oder eine Rechtsvereinbarung handelt):

- ★ ein PEP, ein Familienmitglied oder ein enger Vertrauter eines PEP ist; oder
- ★ Verbindungen zu organisiertem Verbrechen, Drogenhandel, Waffenhandel, Menschenhandel, Korruption ausländischer Beamter, Gewaltverbrechen oder Terrorismus hat; oder
- ★ Verurteilungen oder Anschuldigungen wegen betrügerischer oder krimineller/zweifelhafter Aktivitäten vorliegen oder vorgelegen haben,

Das Unternehmen ist gesetzlich verpflichtet, EDD-Maßnahmen anzuwenden. Der Verwaltungsrat muss eine Entscheidung über die Fortsetzung oder Beendigung der Geschäftsbeziehung treffen (Vorlage siehe Anhang 1). Zu diesem Zweck müssen vollständige Informationen über die Verfügbarkeit von Dokumenten zur Identitätsüberprüfung und die Ergebnisse der Überprüfung vorgelegt werden, damit eine fundierte Entscheidung getroffen werden kann.

Stellt sich bei der Überprüfung heraus, dass ein Kunde oder dessen Grundsätze auf der Sanktionsliste der Vereinten Nationen oder einer vom nationalen Sanktionsausschuss herausgegebenen Liste aufgeführt sind, muss das Unternehmen unverzüglich das nationale Sanktionssekretariat und die FSC benachrichtigen und **der FIU eine STR** gemäß dem Kapitel "Gezielte Finanzsanktionen" dieses Handbuchs übermitteln.

Besteht der begründete Verdacht, dass der Kunde versucht, die Dienste des Unternehmens zu nutzen, um Geldwäsche und Terrorismusfinanzierung zu begehen, muss ein interner Verdachtsbericht an den MLRO übermittelt werden.

10.3 Aufzeichnungen über die laufende Überwachung

Alle Screening-Berichte, der Bericht über die Risikobewertung des Kunden und das Blatt für die laufende Überwachung müssen für die Dauer der Geschäftsbeziehung und für einen Zeitraum von mindestens sieben Jahren nach deren Beendigung aufbewahrt

und in der Akte des jeweiligen Kunden gespeichert werden (unabhängig davon, ob es sich um eine Papier- oder eine Softcopy handelt).

11. Gezielte finanzielle Sanktionen

Der Sicherheitsrat der Vereinten Nationen (UNSC) hat Sanktionen verhängt, um die Verbreitung von Massenvernichtungswaffen und die Finanzierung der Verbreitung zu verhindern und zu bekämpfen. Dazu gehören gezielte Finanzsanktionen gegen bestimmte Personen und Einrichtungen, die mit der Verbreitung von Massenvernichtungswaffen in Verbindung gebracht werden. Alle UN-Mitgliedstaaten sind verpflichtet, diese Maßnahmen umzusetzen.

Das UN-Sanktionsgesetz wurde im Mai 2019 in Mauritius in Kraft gesetzt, um die Umsetzung der vom UN-Sicherheitsrat verhängten gezielten Finanzsanktionen zu ermöglichen.

Gemäß Abschnitt 41 des UN-Sanktionsgesetzes muss das Unternehmen interne Kontrollen und andere Verfahren einführen, die es ihm ermöglichen, seinen Verpflichtungen im Rahmen des UN-Sanktionsgesetzes wirksam nachzukommen. Diese Verpflichtungen können wie folgt kategorisiert werden:

- ★ Überprüfung der Sanktionen
    - Kunden-Screening
    - Transaktionsüberwachung
    - Sanktionsabgleich und Beseitigung von False Positives
- ★ Meldepflichten

11.1 Verpflichtungen zur Sanktionsprüfung

11.1.1 Kunden-Screening

Abschnitt 25 des UN-Sanktionsgesetzes schreibt vor, dass jede meldende Person überprüfen muss, ob die Angaben einer gelisteten Partei mit den Angaben eines Kunden übereinstimmen, und wenn dies der Fall ist, feststellen muss, ob der Kunde Gelder oder andere Vermögenswerte in Mauritius besitzt. Alle Kunden und Transaktionen müssen daher anhand von Sanktionslisten auf mögliche Übereinstimmungen überprüft werden.

Bei der Aufnahme einer neuen Geschäftsbeziehung muss das Unternehmen daher im Rahmen des Screening-Prozesses feststellen, ob der potenzielle Kunde und seine Auftraggeber (falls zutreffend) auf der UN-Sanktionsliste oder einer vom nationalen Sanktionsausschuss herausgegebenen Liste aufgeführt sind oder ob sie mit Personen in Verbindung stehen, die auf solchen Listen aufgeführt sind.

Dies gilt auch für die laufende Überwachung im Laufe der Geschäftsbeziehung mit einem Kunden. Daher prüft das Unternehmen im Rahmen des Screening-Prozesses zum Zwecke der laufenden Überwachung, ob der Kunde und seine Auftraggeber (falls zutreffend) auf der UN-Sanktionsliste oder einer vom Nationalen Sanktionsausschuss herausgegebenen Liste aufgeführt sind oder ob sie mit Personen in Verbindung stehen, die auf solchen Listen aufgeführt sind.

11.1.2 Überwachung von Vorgängen

Bei jeder eingehenden und ausgehenden Transaktion müssen die an der Transaktion beteiligten Parteien (d. h. der Überweisende, der Begünstigte, die Vermittler und alle anderen an der Transaktion beteiligten Parteien) vor der Durchführung

der Transaktion anhand der UN-Sanktionsliste und der vom nationalen Sanktionsausschuss herausgegebenen Liste überprüft werden.

Darüber hinaus müssen bei der Transaktionsüberwachung die folgenden Datenpunkte überprüft werden:

1. Die an der Transaktion beteiligten Parteien (d. h. der Überweisende, der Begünstigte, die zwischengeschalteten Stellen und andere an der Transaktion beteiligte Parteien),
2. Banknamen, Bankleitzahlen und andere Routing Codes und
3. Freitextfelder (z. B. Zahlungsreferenz/Zweckangabe).

Wie bereits in diesem Handbuch erwähnt, stellt es gemäß Abschnitt 23 Absatz 1 des UN-Sanktionsgesetzes eine Straftat dar, mit Geldern/sonstigen Vermögenswerten einer Person zu handeln, die auf der UN-Sanktionsliste oder einer von dem gemäß dem UN-Sanktionsgesetz eingerichteten nationalen Sanktionsausschuss erstellten Liste aufgeführt ist.

Abschnitt 24 verbietet es, Gelder oder andere Vermögenswerte oder finanzielle oder andere damit zusammenhängende Dienstleistungen direkt oder indirekt, ganz oder gemeinsam für oder zu Gunsten einer Person bereitzustellen:

1. eine Person, die auf der UN-Sanktionsliste oder einer vom Nationalen Sanktionsausschuss erstellten Liste aufgeführt ist
2. eine Partei, die im Namen oder auf Anweisung einer der unter Buchstabe a) genannten Personen handelt; oder
3. eine Einrichtung, die sich im Besitz oder unter der direkten oder indirekten Kontrolle einer unter Buchstabe a) genannten Person befindet.

Die Nichteinhaltung von Section 23 (1) und Section 24 stellt eine Straftat dar, die im Falle einer Verurteilung mit einer Geldstrafe von bis zu 5 Millionen Rupien oder dem doppelten Wert der Gelder oder anderer Vermögenswerte, je nachdem, welcher Betrag höher ist, und mit einer Freiheitsstrafe von mindestens drei Jahren geahndet wird.

11.1.3 Sanktionsabgleich und Behebung von Fehlalarmen

Wird während des Screening-Prozesses eine Übereinstimmung festgestellt (d.h. wenn sich herausstellt, dass ein Kunde, ein Auftraggeber eines Kunden oder eine an einer Transaktion beteiligte Person auf der UN-Sanktionsliste oder einer vom nationalen Sanktionsausschuss herausgegebenen Liste aufgeführt ist oder mit einer solchen Person in Verbindung steht), muss das Unternehmen unverzüglich handeln:

- ★ die betreffende Transaktion zu stoppen, um eine Straftat nach Abschnitt 23 des UN-Sanktionsgesetzes zu vermeiden, und
- ★ auf der Grundlage der dem Unternehmen zur Verfügung stehenden Informationen und der in der Sanktionsliste enthaltenen Angaben weitere Nachforschungen anzustellen, um die Übereinstimmung zu bestätigen.

Das Unternehmen führt Aufzeichnungen über Falschmeldungen (durch Einrichtung eines Falschmelderegisters), die den zuständigen Behörden oder geeigneten Dritten (wie dem unabhängigen Prüfer für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung und dem FSC) auf Anfrage zur Verfügung gestellt werden.

11.2 Berichtspflichten

Stellt das Unternehmen eine bestätigte positive Übereinstimmung fest (d. h., die Angaben eines Kunden oder Auftraggebers eines Kunden stimmen mit den Angaben einer Person überein, die auf der UN-Sanktionsliste oder einer vom Nationalen Sanktionsausschuss herausgegebenen Liste aufgeführt ist), ist das Unternehmen gemäß Abschnitt 25(2) des

UN-Sanktionsgesetzes verpflichtet, dem Nationalen Sanktionssekretariat einen Bericht unter Verwendung der Vorlage zu übermitteln, die von der Website des Nationalen Sanktionssekretariats heruntergeladen werden kann - http://nssec.govmu.org an die folgende E-Mail-Adresse nssec@govmu.org.

Die Nichtmeldung ist eine Straftat, die bei Verurteilung mit einer Geldstrafe von bis zu 5 Millionen Rupien und einer Freiheitsstrafe von bis zu 10 Jahren geahndet wird.

Wenn das Unternehmen eine Meldung an das Nationale Sanktionssekretariat gemäß Abschnitt 25(2) vornimmt, muss es dies auch an die FSC melden.
Falls das Unternehmen Gelder oder andere Vermögenswerte einer Person, die auf der UN-Sanktionsliste oder einer vom Nationalen Sanktionsausschuss herausgegebenen Liste aufgeführt ist, hält, kontrolliert oder in seinem Gewahrsam oder Besitz hat, muss es dem Nationalen Sanktionssekretariat gemäß Abschnitt 23(4) unverzüglich Folgendes melden

1. Einzelheiten zu den fraglichen Geldern oder sonstigen Vermögenswerten,
2. Name und Anschrift der Person, die auf der UN-Sanktionsliste oder einer vom nationalen Sanktionsausschuss herausgegebenen Liste steht,
3. Einzelheiten zu jeder versuchten Transaktion mit den Geldern oder sonstigen Vermögenswerten, einschließlich
    a. Name und Anschrift des Absenders;
    b. den Namen und die Anschrift des Empfängers;
    c. den Zweck der versuchten Transaktion;
    d. die Herkunft der Gelder oder sonstigen Vermögenswerte und
    e. wohin die Gelder oder sonstigen Vermögenswerte gesendet werden sollten.

Die Notifizierung muss unter Verwendung der Vorlage erfolgen, die von der Website des Nationalen Sanktionssekretariats - http://nssec.govmu.org - heruntergeladen werden kann und an die folgende E-Mail-Adresse nssec@govmu.org zu übermitteln ist

Die Nichteinhaltung von Abschnitt 23(4) stellt eine Straftat dar und kann gemäß Abschnitt 45 des UN-Sanktionsgesetzes mit einer Geldstrafe von bis zu 1 Million Rupien und einer Freiheitsstrafe von bis zu 10 Jahren geahndet werden.

11.2.1 Einreichung der STR

Gemäß Abschnitt 39 des UN-Sanktionsgesetzes muss das Unternehmen der zentralen Meldestelle unverzüglich eine Verdachtsmeldung übermitteln, wenn es über Informationen in Bezug auf eine Person verfügt, die auf der UN-Sanktionsliste oder einer vom nationalen Sanktionsausschuss herausgegebenen Liste aufgeführt ist. Wenn nach einer Überprüfung festgestellt wird, dass ein Kunde oder ein Auftraggeber eines Kunden auf der UN-Sanktionsliste oder einer vom Nationalen Sanktionsausschuss herausgegebenen Liste aufgeführt ist, muss daher ein interner STR an den MLRO des Unternehmens zur weiteren Bearbeitung übermittelt werden.

11.2.2 Änderungen der UN-Sanktionsliste

Die UN-Sanktionsliste ist dynamisch und kann von Zeit zu Zeit geändert werden, auch durch Ergänzungen. In diesem Fall sendet die FIU eine Mitteilung an alle registrierten MLRO/DMLRO/Meldepflichtigen der obersten Führungsebene, je nach Fall. Nach Erhalt dieser Mitteilungen ist der Compliance Officer verpflichtet:

1. Unverzügliche Überprüfung, ob einer seiner Kunden mit dem Neuzugang übereinstimmt (ein angemessener Nachweis für eine solche Überprüfung ist in den Unterlagen aufzubewahren)

2. die vom Unternehmen verwendete Screening-Engine zu testen, um sicherzustellen, dass ihre Datenbanken umgehend aktualisiert werden
3. Bei Nichtübereinstimmung mit der UN-Sanktionsliste nach Erhalt von Mitteilungen über Änderungen der UN-Sanktionsliste durch die FIU muss das Unternehmen einen NIL-Bericht an die NSS übermitteln und das FSC in der gesendeten E-Mail kopieren.

12. Meldung verdächtiger Transaktionen

Gemäß Abschnitt 14 des FIAMLA ist das Unternehmen gesetzlich verpflichtet, der FIU so schnell wie möglich, spätestens jedoch innerhalb von fünf Arbeitstagen nach dem Tag, an dem es von einer Transaktion Kenntnis erlangt, von der es Grund zu der Annahme hat, dass es sich um eine verdächtige Transaktion handeln könnte, Bericht zu erstatten.

12.1 Was ist eine verdächtige Transaktion?

Abschnitt 2 des FIAMLA definiert eine verdächtige Transaktion als eine Transaktion, die:

1. Anlass zu dem begründeten Verdacht gibt, dass es sich um
    a. das Waschen von Geld oder Erträgen aus einer Straftat; oder
    b. Gelder, die mit der Finanzierung des Terrorismus oder der Finanzierung der Verbreitung von Massenvernichtungswaffen oder anderen Aktivitäten oder Transaktionen im Zusammenhang mit dem Terrorismus im Sinne des Gesetzes zur Verhütung des Terrorismus oder eines anderen Gesetzes in Verbindung stehen oder dafür verwendet werden sollen, unabhängig davon, ob die Gelder Erträge aus einer Straftat darstellen oder nicht;
2. unter ungewöhnlich komplizierten oder ungerechtfertigten Umständen vorgenommen wird;
3. keine wirtschaftliche Rechtfertigung oder kein rechtmäßiges Ziel zu haben scheint;
4. von oder im Namen einer Person getätigt wird, deren Identität nicht zur Zufriedenheit der Person, mit der die Transaktion getätigt wird, festgestellt wurde, oder
5. aus irgendeinem anderen Grund Verdacht erregt.

Zu beachten ist, dass gemäß Abschnitt 2 des FIAMLA eine Transaktion auch eine geplante oder versuchte Transaktion umfasst.

Verdächtige Transaktionen sind Transaktionen, bei denen der begründete Verdacht besteht, dass sie mit der Begehung von Geldwäsche und Terrorismusfinanzierung in Zusammenhang stehen. Der begründete Verdacht richtet sich danach, was unter Berücksichtigung der normalen Geschäftspraktiken und -systeme im Rahmen der Geschäftstätigkeit des Unternehmens und der Branche, in der es tätig ist, angemessen ist. Eine verdächtige Transaktion kann mehrere Faktoren umfassen, die für sich genommen unbedeutend erscheinen, aber in ihrer Gesamtheit den Verdacht aufkommen lassen, dass die Transaktion mit der Begehung oder versuchten Begehung von Geldwäsche und Terrorismusfinanzierung in Zusammenhang steht.

Es gibt keinen Schwellenwert für die Meldung einer verdächtigen Transaktion. Nach Abschnitt 5 des FIAMLA ist es jedoch eine Straftat, eine Barzahlung von mehr als 500 000 Rupien oder einem entsprechenden Betrag in Fremdwährung zu leisten oder anzunehmen. Jede Barzahlung, die 500.000 Rupien oder den entsprechenden Betrag in ausländischer Währung übersteigt, muss gemeldet werden.

Wenn zwei oder mehr Transaktionen in Höhe von insgesamt 500.000 Rupien oder dem entsprechenden Betrag in ausländischer Währung innerhalb eines kurzen Zeitraums im Namen desselben Kunden durchgeführt werden und das Unternehmen weiß, dass diese Transaktionen oder Überweisungen von oder im Namen desselben Kunden durchgeführt werden, müssen sie als eine einzige Transaktion behandelt und der FIU gemeldet werden.

12.2 Indikatoren für verdächtige Transaktionen

Das Unternehmen sollte aufmerksam sein und dafür sorgen, dass alle verdächtigen Indikatoren sofort erkannt werden. Einige Indikatoren sind im Folgenden aufgeführt:

1. Nicht in der Lage sein, die Quelle der Gelder zufriedenstellend zu identifizieren
2. Einzahlungen erfolgen aus Quellen (z. B. Bankkonten), die nicht auf den Namen des Kunden lauten, und auf den Namen einer nicht identifizierten dritten Partei, ohne dass dies begründet wird
3. Das Handelsmuster scheint keinen rechtmäßigen oder wirtschaftlichen Grund zu haben und/oder entspricht nicht dem Kundenprofil
4. Es ist nicht möglich, aktuelle CDD-Informationen über einen Kunden zu erhalten

12.3 Meldepflicht

Eine STR muss bei der FIU eingereicht werden, wenn das Unternehmen nicht alle Informationen erhalten kann, die zur Feststellung der Identität des Kunden erforderlich sind. Das Unternehmen ist verpflichtet, eine STR bei der FIU einzureichen, wenn es nicht in der Lage ist, die erforderlichen EDD-Maßnahmen durchzuführen.

Es liegt in der Verantwortung des MLRO (bzw. in dessen Abwesenheit des DMLRO), STRs an die FIU zu übermitteln. Kein anderer Angestellter oder leitender Angestellter der Gesellschaft darf eine STR an die FIU übermitteln. Damit der MLRO STRs bei der FIU einreichen kann, muss er auf die verdächtige Transaktion aufmerksam gemacht oder darüber informiert werden. Zu diesem Zweck müssen die Angestellten oder leitenden Angestellten verdächtige Transaktionen an den MLRO melden, indem sie einen internen STR einreichen (Vorlage siehe Anhang 3). In Abwesenheit des Hauptrechnungsprüfers ist der stellvertretende Hauptrechnungsprüfer für die Untersuchung und Einreichung von STR-Meldungen zuständig.

12.4 Wann ist ein interner STR an die MLRO zu übermitteln?

Ein Angestellter oder Beamter, der mit den folgenden Fällen konfrontiert wird, muss eine interne Meldung (Vorlage in Anhang 3) an den MLRO machen:

- ★ Die Dokumente zur Identitätsüberprüfung (während des CDD-Prozesses) können für den Kunden und einen seiner Auftraggeber nicht beschafft werden (falls der Kunde eine juristische Person/Rechtsvereinbarung ist),
- ★ Die EDD-Maßnahmen müssen angewendet werden, aber die erforderlichen EDD-Dokumente können nicht beschafft werden,
- ★ Nach der Kundenrisikobewertung wird der Kunde als verboten eingestuft.
- ★ Jeder Verdacht, dass eine Transaktion direkt oder indirekt mit Geldwäsche, Terrorismusfinanzierung oder Proliferationsfinanzierung in Verbindung steht

Interne STRs können entweder persönlich in einem versiegelten Umschlag bei der MLRO eingereicht oder als PDF-Anhang per E-Mail versandt werden. Interne STRs und STRs müssen streng vertraulich behandelt werden.

Sobald die MLRO / DMLRO einen STR erhält, bestätigt sie den Empfang durch eine E-Mail an den betreffenden Mitarbeiter.

12.4.1 Kippen

Sobald der Mitarbeiter einen internen STR an die MLRO gemeldet hat, sollte er sich von der MLRO beraten lassen, wie er mit dem Kunden, für den die verdächtige Transaktion geplant ist oder von dem sie getätigt wurde, umgehen soll, um zu vermeiden, dass der Kunde erfährt, dass die Transaktion gemeldet wurde. Beamte und Angestellte des Unternehmens dürfen den Kunden oder eine andere Person nicht darüber informieren oder warnen, dass ein interner Verdachtsfall an die MLRO gemeldet wurde. Der MLRO ist der Hauptansprechpartner der Gesellschaft für die FIU.

Den leitenden Angestellten und Mitarbeitern des Unternehmens ist es strengstens untersagt, Informationen oder andere Angelegenheiten, die eine Untersuchung einer verdächtigen Transaktion beeinträchtigen könnten, an andere Personen weiterzugeben. Andernfalls kann dies eine Straftat (Tipping Off) nach dem FIAMLA darstellen.

Gemäß Abschnitt 16(1) FIAMLA dürfen das Unternehmen und seine Bediensteten **keine unbefugten Personen** (einschließlich Kollegen) darüber informieren, dass eine Verdachtsmeldung eingereicht wird oder wurde oder dass damit zusammenhängende Informationen von der FIU angefordert, geliefert oder an sie übermittelt werden oder wurden.) Wer gegen Abschnitt 16 (1) verstößt, begeht eine Straftat und wird im Falle einer Verurteilung mit einer Geldstrafe von bis zu 5 Millionen Rupien und einer Freiheitsstrafe von bis zu 10 Jahren bestraft (Abschnitt 16 (3A) FIAMLA).

12.4.2 Umgang mit internen Berichten über verdächtige Transaktionen

Sobald die MLRO einen internen STR erhält, nimmt sie einen Eintrag in das STR-Protokoll (siehe Anhang 4) mit allen Einzelheiten vor und bestätigt den Erhalt per E-Mail an die Person, die den internen STR eingereicht hat.

Die MLRO erhält Zugang zu allen relevanten Informationen oder Aufzeichnungen, um zu beurteilen, ob die Transaktion verdächtig ist oder nicht. Gelangt der MLRO nach der Untersuchung zu dem Schluss, dass es sich um eine verdächtige Transaktion handelt, übermittelt er der FIU so bald wie möglich, spätestens jedoch innerhalb von fünf Arbeitstagen nach dem Tag, an dem der Verdacht aufgekommen ist, einen STR.

Der MLRO dokumentiert im STR-Protokoll die Informationen, die zur Bewertung der gemeldeten Transaktion geprüft wurden, sowie das Datum, an dem die STR an die FIU übermittelt wurde. Wenn der Fall dies rechtfertigt, holt der MLRO den Rat der FIU ein, wie mit der Kundenbeziehung weiter zu verfahren ist oder wie sie zu behandeln ist.

Kommt der MLRO nach der Prüfung zu dem Schluss, dass die gemeldete Transaktion nicht verdächtig ist, dokumentiert er im STR-Protokoll auch die Informationen, die zur Bewertung der Transaktion geprüft wurden, sowie die Gründe, warum er keine Meldung an die FIU erstattet hat. Die Dokumentation der Informationen umfasst das Führen einer (physischen oder elektronischen) Akte, zu der nur der MLRO oder sein Stellvertreter Zugang hat, und die Aufnahme der folgenden Dokumente/Informationen in diese Akte:

- ★ Fakten, die sich auf die mutmaßliche verdächtige Aktivität / Transaktion beziehen
- ★ Dokumente / Beweise / Informationen im Zusammenhang mit der internen Untersuchung durch den MLRO oder den stellvertretenden MLRO
- ★ Ergebnisse der internen Ermittlungen
- ★ Schriftliche Protokolle von Besprechungen mit Mitarbeitern während der internen Ermittlungen (falls vorhanden)
- ★ Schriftliche Analyse des MLRO / stellvertretenden MLRO zur Begründung der Entscheidung, eine Verdachtsmeldung bei der FIU einzureichen oder nicht einzureichen

Die obige Liste ist nicht erschöpfend.

Zusammenfassend kann man sagen, dass die verschiedenen Schritte für die MLRO folgende sind, wenn eine STR von einem Arbeitnehmer eingeht:

- ★ Aktualisierung des STR-Protokolls (Vorlage in Anhang 4) mit dem Datum, an dem er die STR erhalten hat, der Art und anderen relevanten Details;
- ★ weitere Ermittlungen anstellen, ggf. weitere Dokumente/Informationen vom Kunden anfordern (um Hinweise zu vermeiden), Gespräche mit dem Mitarbeiter, der den Kunden betreut, führen usw;
- ★ Entscheidung darüber, ob der STR nach der Untersuchung bei der FIU eingereicht werden soll oder nicht; und
- ★ das STR-Protokoll entsprechend zu aktualisieren.

12.4.3 Einreichung der STR an die FIU

STRs können entweder elektronisch oder manuell an die FIU übermittelt werden.

12.4.3.1 Elektronische Übermittlung von STRs

Die elektronische Übermittlung von STRs kann über die Website der FIU (goAML) auf die folgenden beiden Arten erfolgen:

1. im XML-Format;
2. durch Ausfüllen eines webbasierten Online-Formulars STR auf der GoAML-Plattform

Um STRs über die FIU-Website einreichen zu können, muss der MLRO/DMLRO auf der GoAML-Plattform bei der FIU registriert sein. Ein Nachweis für diese Registrierung ist in den Akten aufzubewahren.

Sobald das Unternehmen registriert, überprüft und von der FIU akzeptiert wurde, kann der MLRO STRs online einreichen.

Die Registrierung muss auf der Website der FIU über die goAML-Anwendung oder auf www.mrugoaml.fiumauritius.org erfolgen, indem Sie auf den Web User Guide für Einzelheiten zur Registrierung klicken. Sowohl der MLRO als auch der DMLRO müssen jederzeit als aktive Nutzer auf der GoAML-Plattform registriert sein.

12.4.3.2 Einreichung von STRs auf Papier

Falls das Unternehmen technisch nicht in der Lage ist, STRs elektronisch zu übermitteln, muss die MLRO:

1. Laden Sie ein leeres STR-Formular von der FIU-Website herunter oder folgen Sie dem unten stehenden Link:
2. http://www.fiumauritius.org/English/Reporting/Documents/STR_FORM_FINAL_VERSION.pdf
3. füllen Sie es aus, und
4. lassen Sie es entweder persönlich am Empfang der FIU im 10. Stock des SICOM Tower, Wall Street, Ebene Cybercity, Ebene 72201, Republik Mauritius, abgeben oder senden Sie es per Fax an +230 466 2431.

13. Screening und Schulung von Mitarbeitern

13.1 Screening der Mitarbeiter:

Es gehört zu den Grundsätzen des Unternehmens, bei der Einstellung von Mitarbeitern oder vor der Ernennung eines Direktors oder leitenden Angestellten (wie im Financial Services Act 2007 definiert) eine Überprüfung der Kandidaten durchzuführen, um sicherzustellen, dass sie kompetent und für die zu besetzende Position geeignet sind. Zu den Überprüfungsmaßnahmen können gehören:

1. Einholung und Bestätigung von Informationen über den beruflichen Werdegang, die Qualifikationen und die beruflichen Mitgliedschaften;
2. Einholen und Bestätigen geeigneter Referenzen;
3. Einholung und Bestätigung von Einzelheiten über etwaige behördliche Maßnahmen oder Maßnahmen eines Berufsverbands gegen den potenziellen Mitarbeiter;
4. Einholen und Bestätigen von Einzelheiten über etwaige strafrechtliche Verurteilungen, einschließlich der Überprüfung des Strafregisters des potenziellen Mitarbeiters; und
5. Abgleich der Mitarbeiter mit der UN-Liste der im Rahmen der gezielten Finanzsanktionen gegen Terrorismus- und Proliferationsfinanzierung benannten Personen

Die Aufzeichnungen über die durchgeführten Untersuchungen werden als Teil der Beschäftigungsdaten jedes Mitarbeiters aufbewahrt.

13.1.1 Laufendes Screening

Das Unternehmen führt ein fortlaufendes Screening-Programm durch, um sicherzustellen, dass bestehende Mitarbeiter während ihrer gesamten Beschäftigungszeit kein Risiko für das Unternehmen darstellen. Dies kann beispielsweise wichtig sein, um zu wissen, ob ein bestehender Mitarbeiter wegen eines Verbrechens verurteilt wurde oder in ein Verhalten verwickelt war, das dem Unternehmen oder seinen Aktivitäten schaden könnte. In diesem Zusammenhang gelten die nachstehenden Maßnahmen für bestehende Mitarbeiter:

- ★ Durchführung eines erneuten Screenings in den einschlägigen Datenbanken für negative Medien und der UN-Sanktionsliste für bestehende Mitarbeiter alle 3 Jahre

13.2 Schulung der Mitarbeiter:

Alle Mitarbeiter, deren Aufgaben sich auf die Abwicklung von Geschäftsbeziehungen oder Transaktionen beziehen, sollten mit den einschlägigen Rechtsvorschriften und Standards zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung vertraut gemacht werden. Das Unternehmen ist daher bestrebt, seine leitenden Angestellten und Mitarbeiter, die an der Abwicklung von Geschäftsbeziehungen oder Transaktionen im Zusammenhang mit den Aktivitäten des Unternehmens beteiligt sind, zu schulen.

Die Mitarbeiter erhalten eine Schulung, die mindestens Folgendes umfasst:

- ★ Rechtliche Verpflichtungen der Gesellschaft gemäß AML-CFT-Gesetzen, -Verordnungen und -Richtlinien;
- ★ die Geldwäsche- und Terrorismusfinanzierungsschwachstellen der von der Gesellschaft angebotenen Produkte und Dienstleistungen;
- ★ Die AML-CFT-Kontrollen und -Verfahren des Unternehmens;

- ★ die Identität und die Verantwortlichkeiten des MLRO;
- ★ Identifizierung und Meldung verdächtiger Transaktionen;
- ★ die strafrechtlichen Sanktionen, die bei Nichtmeldung verdächtiger Transaktionen verhängt werden;
- ★ Neue Entwicklungen, einschließlich Informationen über aktuelle Techniken, Methoden, Trends und Typologien der Geldwäsche und Terrorismusfinanzierung; und
- ★ Informationen über die sich ändernden Verhaltensweisen und Praktiken von Geldwäschern und Terrorismusfinanzierern.

Neue Mitarbeiter, die an der Geschäftstätigkeit des Unternehmens beteiligt sind, erhalten eine AML-CFT-Sensibilisierungsschulung zu den Maßnahmen, die innerhalb des Unternehmens in Bezug auf AML-CFT ergriffen werden, und zu ihren Verpflichtungen als Mitarbeiter/Beamte eines Finanzinstituts gemäß den geltenden gesetzlichen Bestimmungen. Der neue Mitarbeiter erhält eine AML-CFT-Schulung, sobald dies vernünftigerweise praktikabel ist, in jedem Fall aber innerhalb eines Monats nach Beginn des Arbeitsverhältnisses/Vertrags. Die Schulung soll sicherstellen, dass der neue Mitarbeiter/Bedienstete die ihm auferlegten rechtlichen und regulatorischen Verpflichtungen kennt und in der Lage ist, eine verdächtige Transaktion zu erkennen und die Verfahren zu befolgen, um eine verdächtige Transaktion angemessen zu melden.

Darüber hinaus schult das Unternehmen die Mitglieder des Verwaltungsrats und die Mitarbeiter der oberen Führungsebene speziell. Die Schulung muss Folgendes umfassen:

13.2.1 Für den Verwaltungsrat und die leitenden Angestellten

- ★ Straftaten und Sanktionen bei Nichtmeldung oder Unterstützung von Geldwäschern oder an der Terrorismusfinanzierung beteiligten Personen;
- ★ Anforderungen an die CDD, einschließlich der Überprüfung der Identität und der Aufbewahrung von Aufzeichnungen; und
- ★ insbesondere die Anwendung der risikobasierten Strategie und Verfahren des Finanzinstituts.

13.2.2 Für den Compliance-Beauftragten, den MLRO und den stellvertretenden MLRO

1. AML/CFT-Gesetze und -Vorschriften;
2. die internationalen Standards und Anforderungen, auf die sich die Strategie von Mauritius stützt, insbesondere die 40 Empfehlungen der FATF und die Berichte über die ML/TF-Typologie, die für ihre Geschäftstätigkeit relevant sind;
3. die Ermittlung und das Management von ML/TF-Risiken;
4. die Gestaltung und Umsetzung interner Systeme zur Kontrolle von Geldwäsche und Terrorismusfinanzierung;
5. die Konzeption und Umsetzung von Programmen zur Prüfung und Überwachung der Einhaltung der Vorschriften im Bereich Geldwäsche und Terrorismusfinanzierung;
6. die Identifizierung und Behandlung verdächtiger Aktivitäten und Vereinbarungen sowie verdächtiger versuchter Aktivitäten und Vereinbarungen;
7. die Schwachstellen von Geldwäsche und Terrorismusfinanzierung bei den einschlägigen Dienstleistungen und Produkten;
8. den Umgang mit und die Validierung von internen Offenlegungen;
9. das Verfahren zur Einreichung einer externen Meldung;
10. Zusammenarbeit mit den Strafverfolgungsbehörden;
11. Trends und Typologien im Bereich Geldwäsche und Terrorismusfinanzierung; und
12. das Management des Risikos, einen Tipp abzugeben.

Alle Schulungsinformationen sind in das Schulungsprotokoll (Vorlage in Anhang 5) einzutragen.

13.2.3 Obligatorische Teilnahme an der Sensibilisierungsveranstaltung

Wie bereits erwähnt, sind Sensibilisierungsveranstaltungen für Mitarbeiter eine der Methoden, die das Unternehmen gewählt hat, um sein Ziel zu erreichen, das Wissen der Mitarbeiter über AML-CFT aufrechtzuerhalten oder zu erweitern, damit es seine AML-CFT-Verpflichtungen vollständig erfüllen kann. Darüber hinaus werden die Anwesenheit und die Leistung der Mitarbeiter bei den Sensibilisierungsveranstaltungen/Schulungen überwacht. Daher ist die Teilnahme an Sensibilisierungssitzungen obligatorisch, und die Nichtteilnahme ohne angemessene Entschuldigung kann zu angemessenen Disziplinarmaßnahmen seitens des Unternehmens führen.

13.3 Schulung für Compliance-Beauftragte, MLRO und stellvertretende MLRO

Da die MLRO/DMLRO für die ordnungsgemäße Bearbeitung, Bewertung und Meldung verdächtiger Transaktionen an die FIU verantwortlich sind, müssen sie entsprechend geschult werden, damit sie ihre Aufgaben und Pflichten erfüllen können.

Der Compliance Officer ist ein weiterer wichtiger Mitarbeiter, da er für die tägliche Überwachung der Einhaltung der Vorschriften zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung zuständig ist. In diesem Zusammenhang ist es äußerst wichtig, dass der Compliance-Beauftragte, der MLRO und der DMLRO jährlich mindestens 10 Stunden Schulung erhalten, die sich auf ihre spezifische Rolle und Aufgaben gemäß den FIAML-Verordnungen 2018 konzentrieren. Dies steht im Einklang mit den Anforderungen der Competency Standards.

14. Aufbewahrung von Aufzeichnungen

14.1 Identitätsprüfung und Transaktionsaufzeichnungen

Gemäß Verordnung 14 (1) muss das Unternehmen alle Aufzeichnungen über Geschäfte in einer Form aufbewahren und pflegen, die eine rasche Rekonstruktion jedes einzelnen Geschäfts ermöglicht.

Die Gesellschaft ist verpflichtet, Aufzeichnungen über alle Geschäfte, an denen sie beteiligt ist, sowie Aufzeichnungen über alle Kunden zu führen. Dementsprechend muss das Unternehmen aufbewahrt werden:

1. Aufzeichnungen zur Identifizierung von Kunden und wirtschaftlichen Eigentümern (z. B. Kopien oder Aufzeichnungen von amtlichen Ausweispapieren wie Pässen, Personalausweisen, Führerscheinen oder ähnlichen Dokumenten) sowie Geschäftskorrespondenz für einen Zeitraum von mindestens 7 Jahren nach Beendigung der Geschäftsbeziehung,
2. Aufzeichnungen über Transaktionen, sowohl im Inland als auch im Ausland, für einen Zeitraum von 7 Jahren nach Abschluss der Transaktion
3. Aufzeichnungen über alle Berichte über verdächtige Transaktionen, einschließlich der Begleitdokumente
4. Einzelheiten zu allen Aufzeichnungen über alle Änderungen dieses Handbuchs gemäß Abschnitt 17A des FIAMLA 2002.

Das Unternehmen bewahrt daher die nachstehend aufgeführten Aufzeichnungen für einen Zeitraum von mindestens sieben Jahren nach Beendigung oder Kündigung der Geschäftsbeziehung in der jeweiligen Kundenakte auf (in Papierform oder als Softcopy):

- ★ Unterzeichnete Bedingungen und Konditionen
- ★ Dokumente zur Identitätsüberprüfung (einschließlich etwaiger EDD-Dokumente), Screening-Ergebnisse und durchgeführte Kundenrisikobewertung;
- ★ Handelsinformationen
- ★ Korrespondenz im Zusammenhang mit der Transaktion.

In jedem Fall müssen ausreichende Informationen aufgezeichnet werden, um die Rekonstruktion einer Transaktion mit einem Kunden zu ermöglichen.

14.2 Interne und externe Berichte über verdächtige Transaktionen

In Übereinstimmung mit Abschnitt 17F des FIAMLA und der GwG-CFT-Politik des Unternehmens bewahrt der MLRO die folgenden Aufzeichnungen über die eingegangenen internen Verdachtsmeldungen und die eingereichten STR für einen Zeitraum von mindestens sieben Jahren ab dem Datum der Meldung auf:

- ★ interne Berichte über verdächtige Transaktionen, die bei der MLRO eingehen;
- ★ Aufzeichnungen über Maßnahmen, die nach Erhalt interner Berichte über verdächtige Transaktionen ergriffen wurden;
- ★ Aufzeichnungen über Maßnahmen, die ergriffen wurden, um zu beurteilen, ob die gemeldeten Transaktionen verdächtig sind oder nicht;
- ★ Aufzeichnungen über die Informationen, die geprüft wurden, um zu beurteilen, ob die gemeldeten Transaktionen verdächtig sind oder nicht;
- ★ für den Fall, dass die MLRO nach der Prüfung beschlossen hat, keine Meldung an die FIU zu machen, eine Aufzeichnung der Gründe für die Entscheidung, keine Meldung an die FIU zu machen; und

- ★ alle von der MLRO an die zentrale Meldestelle erstatteten Meldungen.

Diese Aufzeichnungen können in Form von Soft- und/oder Hardcopies aufbewahrt werden.

Es wird darauf hingewiesen, dass gemäß Abschnitt 13(5) FIAMLA der Direktor der FIU im Falle einer Meldung an die FIU das Unternehmen schriftlich auffordert, die Aufzeichnungen in Bezug auf diese verdächtige Transaktion für den in der Meldung angegebenen Zeitraum aufzubewahren.

14.3 Schulungsunterlagen

Das Unternehmen führt Aufzeichnungen über alle AML-CFT-Schulungen, die für die Mitarbeiter durchgeführt wurden, wie unten im Schulungsprotokoll aufgeführt (Vorlage siehe Anhang 5):

- ★ die Daten, an denen die AML-CFT-Schulung stattgefunden hat;
- ★ die Art der Schulung, einschließlich Einzelheiten zum Inhalt und zur Art der Durchführung;
- ★ die Namen der Mitarbeiter, die geschult wurden, und
- ★ Kopien der Aufzeichnungen über die kontinuierliche berufliche Weiterentwicklung (CPD) des Compliance-Beauftragten, des MLRO und des stellvertretenden MLRO.

14.3.1 Änderungen der Richtlinien und Verfahren

Das Unternehmen führt schriftliche Aufzeichnungen über alle Änderungen, die an den Grundsätzen und Verfahren zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung vorgenommen werden, wie im FIAMLA 2002 vorgeschrieben. Diese Aufzeichnungen werden in einem Protokoll über die Änderung von Grundsätzen geführt (Vorlage in Anhang 6).

15. Überwachung und Prüfung der Einhaltung

Wie in Vorschrift 31 des FIAMLR vorgesehen, muss das Unternehmen über angemessene Grundsätze und Verfahren für die Überwachung und Prüfung der Einhaltung der einschlägigen AML-CFT-Anforderungen durch das Unternehmen und seine Tätigkeiten verfügen. Die Überwachung und Prüfung der Einhaltung der Vorschriften umfasst Folgendes:

- ★ Prüfung und Überwachung, ob das Unternehmen über solide und dokumentierte Vorkehrungen zur Steuerung der Risiken verfügt, die bei der durchgeführten Bewertung der Geschäftsrisiken ermittelt wurden;
- ★ Unverzügliche Maßnahmen zur Behebung festgestellter Mängel in Bezug auf AML-CFT

Die Prüfung und Überwachung der Einhaltung der geltenden AML-CFT-Anforderungen durch das Unternehmen muss laufend erfolgen, wobei die nachstehenden Punkte bewertet werden sollten:

- ★ die Angemessenheit der ML/TF-Risikobewertung,
- ★ die Angemessenheit der CDD-Strategien, -Verfahren und -Prozesse und ob sie den internen Anforderungen entsprechen,
- ★ die Angemessenheit des risikobasierten Ansatzes in Bezug auf die den Kunden angebotenen Dienstleistungen und geografischen Standorte,
- ★ die Angemessenheit der Schulungen, einschließlich ihres Umfangs, der Genauigkeit der Materialien und des Schulungsplans
- ★ die Einhaltung der geltenden Gesetze,
- ★ die Fähigkeit des Systems, ungewöhnliche Aktivitäten zu erkennen,
- ★ die Angemessenheit der Aufbewahrung von Unterlagen und
- ★ die Überprüfung der Systeme zur Meldung verdächtiger Transaktionen (Suspicious Transaction Reporting, STR), die unter anderem eine Bewertung der Untersuchung und Weiterleitung ungewöhnlicher Transaktionen umfassen sollte.

Der Compliance-Beauftragte ist für die Durchführung der Überwachung und Prüfung der Einhaltung der AML/CFT-Anforderungen gemäß Verordnung 31 verantwortlich. Darüber hinaus sind die Ergebnisse der Überwachung und Prüfung zu dokumentieren und dem Vorstand zu melden, um sicherzustellen, dass der Vorstand eine angemessene Aufsicht über den Stand der Einhaltung und die Wirksamkeit der durchgeführten AML/CFT-Kontrollmaßnahmen hat.

16. Unabhängige AML/CFT-Prüfung

Gemäß Vorschrift 22(1)(d) der FIAML-Verordnungen 2018 ist die Gesellschaft verpflichtet, eine unabhängige Prüfungsfunktion einzurichten, um die Einhaltung und Wirksamkeit der gemäß dem FIAMLA und den FIAML-Verordnungen 2018 getroffenen Maßnahmen zu überprüfen und zu verifizieren.

16.1 Umfang der Prüfung

Die Prüfung sollte mindestens die folgenden Punkte umfassen:

1. die Angemessenheit der ML/TF-Risikobewertung,
2. die Angemessenheit der CDD-Strategien, -Verfahren und -Prozesse und ob sie den internen Anforderungen entsprechen,
3. die Angemessenheit des risikobasierten Ansatzes in Bezug auf die den Kunden angebotenen Dienstleistungen und geografischen Standorte,
4. die Angemessenheit der Schulungen, einschließlich ihres Umfangs, der Genauigkeit der Materialien und des Schulungsplans
5. die Einhaltung der geltenden Gesetze,
6. die Fähigkeit des Systems, ungewöhnliche Aktivitäten zu erkennen,
7. die Angemessenheit der Aufbewahrung von Unterlagen und
8. die Überprüfung der Systeme zur Meldung verdächtiger Transaktionen (Suspicious Transaction Reporting, STR), die unter anderem eine Bewertung der Untersuchung und Weiterleitung ungewöhnlicher Transaktionen umfassen sollte.

16.2 Unabhängigkeit des Abschlussprüfers

Die Prüfung wird von einem internen oder externen Prüfer durchgeführt, der von den Funktionen zur Überwachung der Einhaltung der Vorschriften unabhängig ist, und sollte nicht vom Compliance-Beauftragten durchgeführt werden.

16.3 Ergebnis der Prüfung

Nach der Prüfung legt der Prüfer dem Verwaltungsrat einen Prüfungsbericht vor. Der Bericht deckt den oben genannten Bereich ab, enthält Feststellungen zu festgestellten Mängeln und Qualitätsempfehlungen für sofortige Abhilfemaßnahmen.

Nach Erhalt des Prüfberichts wird ein Aktionsplan aufgestellt, um die bei der Prüfung festgestellten Mängel innerhalb von höchstens einem Monat zu beheben.

16.4 Häufigkeit der Prüfung

Die unabhängige Prüfung wird mindestens einmal jährlich durchgeführt, und alle Berichte sind aufzubewahren und der FIU auf Verlangen vorzulegen. Diese Häufigkeit kann vom Verwaltungsrat in Abhängigkeit von den ML/TF-Risiken, denen das Unternehmen ausgesetzt ist, geändert werden.

Die Prüfungsberichte werden dem Verwaltungsrat zur Überprüfung, Genehmigung und für weitere Maßnahmen vorgelegt.

17. Abhängigkeit von Dritten

Gemäß Vorschrift 21 der FIAMLR 2018 kann sich die Gesellschaft bei der Einführung von Geschäften oder der Durchführung von CDD-Maßnahmen im Namen der Gesellschaft auf einen Dritten verlassen. Falls sich die Gesellschaft bei der Geschäftsanbahnung oder der Durchführung von CDD-Maßnahmen in ihrem Namen auf einen Dritten verlässt, muss die Gesellschaft:

1. Maßnahmen ergreifen, um sich zu vergewissern, dass Kopien der Identifikationsdaten und anderer relevanter Unterlagen im Zusammenhang mit den CDD-Anforderungen von der dritten Partei auf Anfrage unverzüglich zur Verfügung gestellt werden;
2. sich zu vergewissern, dass der Dritte reguliert und beaufsichtigt oder für die Zwecke der Bekämpfung von Geldwäsche und Terrorismusfinanzierung überwacht wird und über Maßnahmen zur Einhaltung der CDD- und Aufzeichnungsanforderungen im Einklang mit dem Gesetz und diesen Vorschriften verfügt.

Das Unternehmen darf sich nicht auf einen Dritten verlassen, der in einem Hochrisikoland ansässig ist.

Selbst wenn das Unternehmen einen Dritten mit der Durchführung eines Teils oder der Gesamtheit der CDD-Maßnahmen in seinem Namen beauftragt, muss das Unternehmen sofortigen Zugang zu allen CDD-Dokumenten haben, die entsprechend aufzubewahren sind.

Alle gemäß diesem Absatz unternommenen Schritte (z. B. die Bewertung des aufsichtsrechtlichen Status des Dritten) sind aufzuzeichnen, um die Einhaltung der Verordnung 21 des FIAMLR 2018 nachweisen zu können.

17.1 Risikobewertung und Due-Diligence-Prüfung von Drittanbietern

Das Unternehmen führt eine Risikobewertung und eine Due-Diligence-Prüfung von Drittanbietern durch, die kritische Dienstleistungen für das Unternehmen erbringen, einschließlich ausgelagerter Funktionen wie die Compliance-Funktion, MLRO und DMLRO. Die Risikobewertung und die Due-Diligence-Prüfung haben vor allem folgende Ziele:

1. Identifizierung und Überprüfung der Identität des Drittdienstleisters durch Einholung einschlägiger Informationen und Dokumente aus unabhängigen Quellen
2. Durchführung eines Screenings des Drittdienstleisters, um zu überprüfen, ob es Treffer bei ihm gibt
3. Durchführung einer Risikobewertung des Drittdienstleisters
4. Durchführung einer fortlaufenden Risikobewertung und Sorgfaltsprüfung des Drittdienstleisters

18. Hochrisiko-Länder

Gemäß Vorschrift 12(1)(c) der FIAML-Verordnungen 2018 muss eine meldepflichtige Person verstärkte CDD-Maßnahmen wie hier beschrieben anwenden. Darüber hinaus sieht Vorschrift 24(1) vor, dass bei der Ermittlung von Ländern mit hohem Risiko die folgenden Punkte gebührend zu berücksichtigen sind:

1. strategische Mängel im rechtlichen und institutionellen Rahmen für die Bekämpfung der Geldwäsche und der Terrorismusfinanzierung, insbesondere in Bezug auf
    a. Kriminalisierung von Geldwäsche und Terrorismusfinanzierung;
    b. Maßnahmen im Zusammenhang mit der CDD;
    c. Anforderungen in Bezug auf die Aufbewahrung von Aufzeichnungen;
    d. Anforderungen zur Meldung verdächtiger Transaktionen;
    e. die Verfügbarkeit von genauen und rechtzeitigen Informationen über das wirtschaftliche Eigentum von juristischen Personen und Vereinbarungen für die zuständigen Behörden;

2. die Befugnisse und Verfahren der zuständigen Behörden des Landes zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung, einschließlich angemessener, wirksamer, verhältnismäßiger und abschreckender Sanktionen, sowie die Praxis des Landes bei der Zusammenarbeit und dem Informationsaustausch mit den zuständigen Behörden im Ausland;

3. die Wirksamkeit des Systems des Landes zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung bei der Bewältigung von Risiken der Geldwäsche oder Terrorismusfinanzierung.

Im Hinblick auf die Identifizierung von Hochrisikoländern und in Übereinstimmung mit Regulation 24(3) der FIAML Regulations 2018 wendet die Gesellschaft verstärkte Sorgfaltspflichten in Bezug auf alle Länder an, die von der Financial Action Task Force (FATF) auf ihrer Liste der Länder mit verstärkter Überwachung aufgeführt sind. Es wird darauf hingewiesen, dass die Gesellschaft keine Geschäfte mit Ländern tätigen darf, die auf der Liste der Länder stehen, die von der FATF zu Maßnahmen aufgefordert werden.

Anhang 1 - Genehmigungsformular für die Geschäftsleitung (Hochrisikokunden)

Name des Kunden	
Datum des Onboarding (falls zutreffend)	
Risiko-Einstufung	Hoch
Gründe für das hohe Risiko	
Sonstige Kommentare	

Die Aufnahme oder Fortführung der Geschäftsbeziehung wird hiermit bestätigt:
Zutreffendes bitte ankreuzen

Genehmigt ☐ **Abgelehnt** ☐

Name: _____

Unterschrift: _____

Datum: _____

Anhang 2 - Formular für die laufende Überwachung

Bitte gesondert ansehen

Anhang 3 - Interner Bericht über verdächtige Transaktionen

Interner Bericht über verdächtige Transaktionen (STR)

Einzelheiten der verdächtigen Geschäftsbeziehung

Name des Kunden: _____

Art der dem Kunden angebotenen Dienstleistung: _____

Datum der Aufnahme der Geschäftsbeziehung (tt/mm/jj): _____

Einzelheiten des Verdachts (bitte fügen Sie entsprechende Belege bei)

Verdächtige Transaktion:

_____

Gründe für die Verdächtigung:

_____

Es ist eine Straftat, den Kunden oder eine andere Person über Ihren Verdacht und diesen Bericht zu informieren. Diese Meldung ist als streng zu behandeln **VERTRAULICH.**

Unterschrift des Reporters: _____ Datum (tt/mm/jj): _____

Name des Reporters: _____

FOR MLRO's USE

Date received: **Time**:

Details of Action: (*please attach relevant documents*)

Date assessment completed:
STR submitted to FIU (*please indicate YES/NO*):

Anhang 4 - Protokoll über verdächtige Transaktionen (Suspicious Transaction Report)

Intern - Protokoll des Berichts über verdächtige Transaktionen								
Datum	**STR Ausgefüllt am** (Name der Kundendatei)	**Name des Mitarbeiters, der STR ausfüllt** (mit Angabe der Position)	**Gründe für Internat STR**	**Von der MLRO oder DMLRO entgegengenommen**	**MLRO hat STR bei FIU eingereicht** (Ja / Nein)	**Gründe für die Einreichung bei der FIU** (falls zutreffend)	**Datum der Einreichung bei der FIU (**falls zutreffend)	**Rückmeldung von FIU** (falls zutreffend)

Anhang 5 - Ausbildungsprotokoll

Bitte gesondert ansehen

Anhang 6 - Protokoll zur Änderung der Politik

Bitte gesondert ansehen

Anhang 7 - Bewertung der Unternehmensrisiken und Methodik

Bitte gesondert ansehen

Anhang 8 - Kundenrisikobewertung und Methodik

Bitte gesondert ansehen

Anhang 9 - Anerkennungsformular

Bitte gesondert ansehen

Anhang 10 - Protokoll über politisch exponierte Personen (PEP)

Bitte gesondert ansehen