NORDKOMMERZ

Richtlinie zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung

Aktualisiert am 24. Juni 2025

1. EINFÜHRUNG

1.1. Das Unternehmen bekämpft jegliche Form von Geldwäsche, Terrorismusfinanzierung od er kriminellen Aktivitäten mit großem Engagement und unter strikter Einhaltung der jeweils g eltenden gesetzlichen Vorschriften.

1.2. Unser Money Laundering Reporting Officer („Beauftragter“) und andere Compliance-Fü hrungskräfte sind damit beschäftigt, die entsprechenden Richtlinien und Verfahren zur Bekäm pfung von Geldwäsche und Terrorismusfinanzierung („AML und CTF“) umzusetzen. Diese A ML- und CTF-Richtlinie deckt Verfahren und Prozesse ab:

> (a) zu den Sorgfaltspflichten des Kunden; (b) zur Umsetzung der Aufzeichnungspflich ten; (c) zu den Berichtspflichten; (d) um unsere Führungskräfte und Mitarbeiter über Geldwäsche und Terrorismusfinanzierung sowie über die Richtlinien, Prozesse, Verfah ren und Systeme zu informieren, die wir zur Bekämpfung von Geldwäsche und Terrori smusfinanzierung eingeführt haben; (e) um unsere Führungskräfte und Mitarbeiter dar in zu schulen, Geldwäsche und Terrorismusfinanzierung zu erkennen und damit umzug ehen; (f) die leitenden Angestellten und Mitarbeiter des Unternehmens zu überprüfen, um sicherzustellen, dass sie über die nötige Eignung und Eignung für Aufgaben im Zu sammenhang mit der Bekämpfung von Geldwäsche und Terrorismusfinanzierung verf ügen; (g) zur Rolle und Verantwortung des Beamten; (h) über die Einrichtung einer u nabhängigen Prüffunktion, die ihre AML- und CTF-Prozesse, -Verfahren und -System e testen kann; und (i) über die Einführung von Systemen durch uns im Umgang mit Ge ldwäsche und Terrorismusfinanzierung.

1.3. Das Unternehmen hat eine Reihe von AML-Verfahren eingeführt und wird unsere AML- und Know-Your-Client („KYC“)-Verfahren bei allen Transaktionen anwenden. Wir werden al le angemessenen Maßnahmen ergreifen, um sicherzustellen, dass ein angemessener Schutz bes teht, um einen Verstoß gegen die geltenden Gesetze und Vorschriften bei der Verhinderung un d Eindämmung von Aktivitäten zur Geldwäsche und Terrorismusfinanzierung („ML und TF“) zu verhindern. Die Einhaltung des AML- und CTF-Systems war schon immer unsere höchste Priorität, um den Ruf unseres Unternehmens in der globalen Finanzbranche und bei den Aufsi chtsbehörden zu wahren.

1.4. Bei der Implementierung unserer AML- und CTF-Systeme sowie zur Erkennung von ML - und TF-Risiken verfolgen wir einen risikobasierten Ansatz. Wir werden unsere AML- und C TF-Systeme und -Richtlinien mindestens einmal jährlich aktualisieren, um neue und aufkomm ende Risiken zu berücksichtigen, und dabei Folgendes berücksichtigen:

> (a) die Art und das Ausmaß des Geldwäsche- und Terrorismusfinanzierungsrisikos, mit dem wir im Rahmen unserer Geschäftstätigkeit vernünftigerweise rechnen können; (b) die Art, Größe und Komplexität unseres Geschäfts; (c) Entwicklung neuer Produkte un d neuer Geschäftspraktiken, einschließlich neuer Bereitstellungsmechanismen; und (d) Einsatz neuer oder sich entwickelnder Technologien sowohl für neue als auch für bereit s bestehende Produkte.

2. DEFINITIONEN UND INTERPRETATIONEN

2.1. Die folgenden Begriffe haben folgende Bedeutung:

(a) „Geltende Gesetze und Vorschriften" bedeutet: (i) Gesetze, Regeln oder Anordnung en der zuständigen Regulierungsbehörden; (ii) Gesetze, Regeln oder Anordnungen der zuständigen Regulierungsbehörden in der Gerichtsbarkeit des Kunden; (iii) die Regeln des jeweiligen Finanzmarktes; und (iv) alle anderen für diese Richtlinie geltenden Ges etze (und jeweils in der jeweils gültigen Fassung).

soweit für diese Richtlinie anwendbar).

(c) „Politisch exponierte Person" oder „PEP" bezeichnet eine Person, die mit wichtigen öffentlichen Ämtern betraut ist oder war, wie z. B. dem Staatsoberhaupt, dem Premier minister, Ministern, hochrangigen Politikern, hochrangigen Regierungsbeamten, Justiz - oder Militärbeamten, hochrangigen Führungskräften staatlicher Unternehmen oder in ternationaler Organisationen und Beamten einer politischen Partei.

(d) „Erträge aus Straftaten" sind Vermögenswerte, die direkt oder indirekt aus einer sc hweren Straftat stammen oder verwertet werden, einschließlich:

(i) Eigentum, in das unmittelbar aus der Straftat abgeleitetes oder verwertetes Ei gentum später sukzessive umgewandelt oder umgewandelt wird; und (ii) Einkom men, Kapital oder andere wirtschaftliche Gewinne, die seit der Straftat aus diese m Vermögen erzielt oder realisiert wurden.

Wenn Vermögensgegenstände, bei denen es sich um Erträge aus Straftaten ha ndelt (die ursprünglichen Erträge), mit anderen Vermögensgegenständen ver mischt sind, von denen sie nicht ohne weiteres getrennt werden können, wird der Anteil der Gesamtheit, der durch die ursprünglichen Erträge repräsentiert wird, als Erträge aus Straftaten angesehen.

(e) „Proliferationsfinanzierung" bedeutet die Bereitstellung von Geldern oder Finanzdi enstleistungen, die ganz oder teilweise für die Herstellung, den Erwerb, den Besitz, die Entwicklung, die Ausfuhr, den Umschlag, die Vermittlung, den Transport, die Übertra gung, die Lagerung oder den Einsatz nuklearer, chemischer oder biologischer Waffen und ihrer Trägermittel sowie verwandter Materialien (einschließlich Technologien und Güter mit doppeltem Verwendungszweck, die für nicht legitime Zwecke verwendet we rden) verwendet werden und dabei gegen nationale Gesetze oder gegebenenfalls intern ationale Verpflichtungen verstoßen.

(f) „Zuständige Regulierungsbehörden" bezeichnet die relevante Regulierungsbehörde, die für den Geschäftsbetrieb und die Dienstleister des Unternehmens gelten kann, eins chließlich, aber nicht beschränkt auf die United States Securities and Exchange Comm ission, die United States Financial Industry Regulatory Authority, die United Kingdom Financial Conduct Authority und die Australian

Securities & Investments Commission, die Europäische Wertpapier- und Marktkommission

Behörde, die Mauritius Financial Services Commission, die Vanuatu Financial Services Commission usw. (g) „Quelle des Vermögens" bezieht sich auf die Herkunft d es gesamten Vermögens einer Person (d. h. des Gesamtvermögens). (h) „Quelle der Mi ttel" bezieht sich auf die Herkunft der jeweiligen Gelder oder sonstigen Vermögenswert e, die Gegenstand der Geschäftsbeziehung zwischen einer Person und uns sind (z. B. di e Beträge, die im Rahmen der Geschäftsbeziehung investiert, eingezahlt oder überwiese n werden). (i) „Terrorismusfinanzierung" oder „Terrorismusfinanzierung" bedeutet: (i) die direkte oder indirekte Bereitstellung oder Einziehung von Eigentum auf beliebige Weise: (aa) mit der Absicht, das Eigentum zu nutzen; oder (ab) im Wissen, dass die Im mobilie ganz oder teilweise zur Begehung einer oder mehrerer terroristischer Handlung en genutzt wird (unabhängig davon, ob die Immobilie auf diese Weise genutzt wird ode r nicht); (ii) die Bereitstellung von Eigentum oder finanziellen (oder damit verbundene n) Dienstleistungen auf beliebige Weise, direkt oder indirekt, für oder zu Gunsten einer Person, die dies weiß oder sich nicht darüber im Klaren ist, ob die Person ein Terrorist oder ein mit Terroristen verbundener Mensch ist; oder (iii) das Einsammeln von Eigent um oder das Anwerben von finanziellen (oder verwandten) Dienstleistungen, auf welch e Weise auch immer, direkt oder indirekt, zum Nutzen einer Person, die dies weiß oder unvorsichtig ist, ob die Person ein Terrorist oder ein mit Terroristen verbundener Mens ch ist.

3. GELDWÄSCHE

3.1. Die Phasen der Geldwäsche sind wie folgt:

(a) Platzierung – Veräußerung von Gelderlösen aus illegalen Aktivitäten; (b) Schichtu ng – Trennung illegaler Erträge von ihrer Quelle durch die Schaffung komplexer Schic hten von Finanztransaktionen, die darauf abzielen, die Herkunft des Geldes zu verschle iern, den Prüfpfad zu untergraben und Anonymität zu gewährleisten; und (c) Integratio n – Erweckung des Eindrucks der scheinbaren Legitimität von kriminell (d) erlangtem Reichtum. In Situationen, in denen der Schichtungsprozess erfolgreich ist, führen Inte grationsprogramme die gewaschenen Erlöse effektiv in das allgemeine Finanzsystem z urück und die Erlöse scheinen das Ergebnis legitimer Geschäftsaktivitäten zu sein oder damit in Zusammenhang zu stehen.

3.2. Zu den möglichen Anzeichen von Geldwäsche gehören unter anderem die folgenden:

(a) Zurückhaltung der Kunden, Informationen bereitzustelle n; (b) unvollständige oder inkonsistente Informationen von Kunden; (c) unregelmäßige Geldtransfers und Transaktion en; (d) ungeklärte Investitionen Dritter; (e) Transaktionen mit ungewöhnlich hohem Volumen;

(f) Finanzierungsquelle aus schlecht regulierten Quellen; (g) Transaktionen ohne erkennbaren legitimen oder wirtschaftlichen Zweck; (h) Transaktionen, die unnötig komplex sind; (i) Der Lebensstil des Klienten scheint über die bekannten Einkommensquellen hinauszugehen; (j) die Unternehmensstruktur ist unnötig kompliziert; (k) Nutzung von Bankkonten ohne triftigen Grund; (l) der Kunde scheint als Vertreter einer anderen juristischen Person oder Einzelperson zu handeln, verschweigt jedoch die Identität einer anderen Identität; (m) der Kunde verfügt über mehrere Konten unter einem oder mehreren Namen mit einer großen Anzahl von Überweisungen zwischen Konten; (n) der Kunde zahlt Geld ein, gefolgt von einer Aufforderung, das Geld abzuheben.

4. KUNDEN-DUE-DILIGENCE („CDD“)

4.1. Das Unternehmen hat eine KYC-Richtlinie eingeführt, um die Identität aller unserer Kunden zu überprüfen und eine Kunden-Due-Diligence-Prüfung („CDD“) durchzuführen. Wir führen einen fortlaufenden Due-Diligence-Prozess durch, um das Konto, die Dienstleistung oder die Beziehung unserer Kunden zu jedem unserer Kunden zu überwachen, um das Risiko zu identifizieren, zu mindern und zu verwalten, dem sie gegenüber ihren Kunden ausgesetzt sein könnten, das Geldwäsche, Terrorismusfinanzierung oder andere schwerwiegende Straftaten beinhalten könnte.

4.2. Wir führen CDD durch, wenn eine Person: (a) ein Konto bei uns eröffnet; (b) unsere Dienste in Anspruch nimmt; oder (c) eine Geschäftsbeziehung mit uns eingeht.

4.3. Wir führen CDD durch für: (a) eine Person, die eine Transaktion durchführt; (b) eine Person, in deren Namen eine Transaktion durchgeführt wird; und (c) ein wirtschaftlicher Eigentümer;

wenn wir berechtigten Grund zu der Annahme haben, dass die Person eine Transaktion im Namen einer anderen Person durchführt. Wir prüfen, ob eine Person berechtigt ist, die betreffende Transaktion im Namen der anderen Person vorzunehmen.

4.4. Darüber hinaus führen wir CDD beim Kunden durch:

(a) vor Aufnahme einer Geschäftsbeziehung mit dem Kunden; (b) vor der Ausführung für den Kunden oder wenn der Kunde eine gelegentliche Transaktion durchführt, bei der es sich um einen Betrag handelt, der einem Gesamtwert von 2.000,00 USD oder dem Gegenwert in Fremdwährung entspricht oder diesen übersteigt, für eine große Bargeldtransaktion oder einen internationalen Währungstransfer, unabhängig davon, ob sie in einem einzigen Vorgang oder in mehreren Vorgängen durchgeführt wird, wenn wir vernünftigerweise annehmen, dass sie miteinander verbunden sind. Bei der Feststellung, ob die Transaktionen miteinander verbunden sind, berücksichtigen wir die Faktoren in Abschnitt 9.6 im Vergleich zum Zeitrahmen, innerhalb dessen die Transaktionen durchgeführt werden; (c) wenn wir von zuständigen Aufsichtsbehörden, Zahlungsdienstleistern oder Dienstleistern aufgefordert werden, eine entsprechende CDD durchzuführen; (d) wenn wir für den Kunden eine elektronische Währungsüberweisung durchführen;

(e) wenn wir vermuten, dass der Kunde an Erträgen aus Straftaten, der Finanzierung vo n Terrorismus oder einer schweren Straftat beteiligt ist, unabhängig von der Transaktio nsebene von 4.4(b) oben; (f) wenn wir vermuten, dass die Geldquelle des Kunden von einem Dritten stammt; (g) wenn wir vermuten, dass es sich bei der Transaktion um Ertr äge aus Straftaten handelt oder dass sie zur Finanzierung von Terrorismus oder zur Beg ehung einer schweren Straftat verwendet werden könnte; oder (h) wenn wir Zweifel an der Richtigkeit oder Angemessenheit der Kundenidentifikation oder der zuvor erhaltene n Informationen haben, (i) wenn wir unsere reguläre CDD-Routine durchführen.

4.5. Erforderliche Dokumentenliste

4.5.1. Wenn es sich bei dem Kunden um eine Einzelperson handelt, erfassen wir die f olgenden Informationen: (a) den vollständigen Namen des Kunden; (b) das Geburtsdat um des Kunden; (c) die Wohnadresse des Kunden; (d) der Beruf des Kunden; (e) das /die Staatsangehörigkeitsland(e) des Kunden; (f) das/die Wohnsitzland(e) des Kunden; (g) der Beruf oder die Geschäftstätigkeit des Kunden; (h) die Art und der Zweck der g eplanten Beziehung des Kunden mit uns, einschließlich: (i) der Zweck bestimmter Tra nsaktionen; oder (ii) die erwartete Art und das Ausmaß des Transaktionsverhaltens; (i) Genehmigung einer Person, die vorgibt, für oder im Namen des Kunden zu handeln; (j) die dem Kunden zur Verfügung stehenden Einkünfte oder Vermögenswerte; (k) die Geldquelle des Kunden, einschließlich der Herkunft der Gelder; (l) die Finanzlage des Kunden; (m) das wirtschaftliche Eigentum an den vom Kunden verwendeten Mitteln; und (n) die Begünstigten der von uns im Namen des Kunden vermittelten Transaktione n, einschließlich der Bestimmung der Gelder.

4.5.2. Wenn es sich bei dem Kunden um eine im Ausland eingetragene juristische Per son handelt, erfassen wir die folgenden Informationen:

(a) vollständiger Name des ausländischen Unternehmens; (b) das Land der R egistrierung und vollständige Registrierungsdetails des Kunden; (c) die vollst ändige Adresse des Hauptgeschäftssitzes und der eingetragenen Adresse des Unternehmens; (d) die Unternehmensstruktur; (e) Name jedes Unternehmen sdirektors und Sekretärs; (f) Art der vom Unternehmen durchgeführten Gesc häftstätigkeit; (g) Name und Anschrift der wirtschaftlichen Eigentümer des U nternehmens und der Kontrollstruktur;

(h) das Land, in dem das Unternehmen gegründet, eingetragen oder registriert wurde; (i) die Bestimmungen zur Regelung der Bindungsbefugnis des Kunde n; (j) die Autorisierung jeder Person, die vorgibt, für oder im Namen des Kun den zu handeln, und die Identität der Personen; und (k) den Zweck und die be absichtigte Art der Geschäftsbeziehung mit uns.

4.6. Wir verbieten strengstens den Aufbau einer Geschäftsbeziehung mit Kunden unter falsch en, fiktiven oder irreführenden Namen und werden Aufzeichnungen darüber führen, ob einer u nserer Kunden einen anderen Namen verwendet, unter dem der Kunde allgemein bekannt ist.

4.7. Wir werden von Fall zu Fall alle Kunden prüfen, von denen vernünftigerweise nicht erwa rtet werden kann, dass sie die üblichen Identitätsnachweise vorlegen, und werden versuchen, u ns auf die Verwendung anderer Identitätsnachweise zu einigen, damit Kunden nicht unangeme ssen der Zugang zu den Produkten und Dienstleistungen verweigert wird. Für den Fall, dass hi nreichend nachgewiesen wird, dass Zweifel an der Identifizierung und Verifizierung der wirts chaftlichen Eigentümer bestehen, können wir gemäß dieser AML- und CTF-Richtlinie CDD b ei den leitenden Angestellten des Kunden durchführen.

5. KUNDENRISIKOBEWERTUNG („CRA“)

5.1. Das Unternehmen wird die CRA nach dem risikobasierten Ansatz durchführen. Wir bewe rten das Risiko für jeden Kunden unter Berücksichtigung spezifischer Produkte, Dienstleistun gen, Kunden, Unternehmen, Anzahl der Transaktionen, Transaktionsvolumen, Art der Kunden beziehungen, geografische Standorte, Zweck des Kontos oder der Beziehung, Höhe der beteili gten Vermögenswerte, Umfang der durchzuführenden Transaktionen und Regelmäßigkeit ode r Dauer der Geschäftsbeziehung.

5.2. Wir akzeptieren keine Kunden mit hohem Risiko, die wie folgt identifiziert werden:

Kunden, deren Geschäft große Mengen an Bargeld abwickelt oder komplexe, ungewö hnlich große Transaktionen durchführt, die nicht verifiziert werden konnten.

Kunden mit großen einmaligen Transaktionen oder mehreren Transaktionen, die inner halb kurzer Zeit über dasselbe Konto ausgeführt werden.

Kunden, die ihren Sitz in einer Gerichtsbarkeit mit hohem Risiko oder einer Gerichtsb arkeit mit einem bekanntermaßen höheren Maß an Korruption, organisierter Kriminal ität, Herstellung, Vertrieb, Lagerung oder Erwerb von Waffen oder Drogen haben ode r dort Geschäfte tätigen.

Kunden, die unter die Definition von PEP fallen.

Transaktionen mit den Quellfonds, die nicht überprüft werden können.

Transaktionen ohne ersichtlichen wirtschaftlichen oder legitimen Zweck.

Transaktionen, die die Anonymität begünstigen könnten.

5.3. Wir führen in der Anfangsphase der CDD eine Kundenrisikobewertung durch, um den U mfang der CDD-Maßnahmen und der laufenden Überwachungsmaßnahmen zu bestimmen. A nschließend verfolgen wir einen risikobasierten Ansatz und führen eine kontinuierliche Überw achung der Geschäftsbeziehungen mit Kunden durch, um Geldwäsche- und Terrorismusfinanz ierungsrisiken zu verwalten und zu mindern, und stellen sicher, dass alle damit verbundenen I nformationen aktualisiert werden. Der Rahmen zur Kundenrisikobewertung muss im Verhältn is zur Art und Größe der Geschäfte des Unternehmens mit Kunden stehen.

5.4. Wenn wir einen begründeten Verdacht haben, ist der Kunde verpflichtet, die Quelle oder das Ziel der Transaktionen zu identifizieren und zu überprüfen.

5.5. Zu unseren Schritten zur Durchführung der institutionellen Risikobewertung von Geldwä sche/Terrorismusfinanzierung gehören:

(a) Dokumentation des Risikobewertungsprozesses, der die Identifizierung und Bewert ung relevanter Risiken umfasst, unterstützt durch qualitative und quantitative Analysen und Informationen aus relevanten internen und externen Quellen; (b) Berücksichtigung aller relevanten Risikofaktoren vor der Bestimmung des Gesamtrisikos sowie des geeig neten Ausmaßes und der Art der anzuwendenden Risikominderung; (c) Einholen der Z ustimmung der Geschäftsleitung zu den Ergebnissen der Risikobewertung; (d) über ein en Prozess verfügen, mit dem die Risikobewertung auf dem neuesten Stand gehalten wi rd; und (e) über geeignete Mechanismen verfügen, um die Risikobewertung den zustän digen Regulierungsbehörden bei Bedarf zur Verfügung zu stellen.

6. VEREINFACHTE DUE DILIGENCE („SDD“)

6.1. Wenn das Unternehmen festgestellt hat, dass die Risiken von Geldwäsche und Terrorism usfinanzierung gering sind, kann das Unternehmen einen vereinfachten Due-Diligence-Ansatz („SDD“) anwenden.

6.2. Kunden, auf die SDD angewendet werden kann, sind:

(a) ein Finanzinstitut; (b) eine Einrichtung, die: (i) in einer gleichwertigen Gerichtsbar keit eingetragen oder niedergelassen ist; (ii) ein Geschäft betreibt, das dem eines Fina nzinstituts ähnelt; (iii) die Einhaltung dieser Anforderungen durch eine Behörde in die sem Rechtsgebiet überwacht wird, die ähnliche Funktionen wie die Regulierungsbehör den ausübt; (c) ein an einer Börse notiertes Unternehmen; (d) ein Anlagevehikel, bei dem die Person, die für die Durchführung von Maßnahmen, die den CDD-Maßnahmen in Bezug auf alle Anleger des Anlagevehikels ähneln, verantwortlich ist: (i) ein Finanzi nstitut; (ii) eine eingetragene oder gegründete Einrichtung, die:

verfügt über Maßnahmen, um die Einhaltung von Anforderungen siche rzustellen, die denen der geltenden Gesetze und Verordnungen ähneln; Und

wird auf die Einhaltung dieser Anforderungen überwacht. (e) die Regi erung oder eine öffentliche Einrichtung; oder (f) die Regierung einer gleichwertigen G erichtsbarkeit oder eine Stelle in einer gleichwertigen Gerichtsbarkeit, die ähnliche Fun ktionen wie eine öffentliche Stelle wahrnimmt.

6.3. Im Falle von SDD werden wir:

(a) den Kunden identifizieren und seine Identität überprüfen;

(b) wenn eine Geschäftsbeziehung begründet werden soll und deren Zweck und beabsichtigte Art nicht erkennbar sind, Informationen über den Zweck und die beabsichtigte Art der Geschäftsbeziehung mit uns einholen; und (c) wenn eine Person vorgibt, im Namen des Kunden zu handeln, (i) die Person identifizieren und angemessene Maßnahmen ergreifen, um die Identität der Person zu überprüfen; und (ii) die Befugnis der Person überprüfen, im Namen des Kunden zu handeln.

7. VERSTÄRKTE DUE DILIGENCE („EDD“)

7.1. Wenn das Unternehmen feststellt, dass die Risiken für Geldwäsche und Terrorismusfinanzierung hoch sind, wird das Unternehmen einen erweiterten Due-Diligence-Ansatz („EDD“) und eine verbesserte laufende Überwachung anwenden. Vor der Aufnahme oder Fortsetzung einer Geschäftsbeziehung und/oder Transaktion mit Kunden mit hohem Risiko ist die Genehmigung der Geschäftsleitung von Richmond erforderlich.

7.2. Zu den Hochrisikosituationen, für die EDD gilt, gehören: (a) Kundenrisikofaktor: (i) die Geschäftsbeziehung wird unter ungewöhnlichen Umständen geführt (z. B. erhebliche unerklärliche geografische Unterschiede zwischen uns und dem Kunden); (ii) juristische Personen oder Rechtsvereinbarungen, die ein Shell-Fahrzeug ohne klaren und legitimen kommerziellen Zweck betreffen; (iii) Unternehmen, die Nominee-Aktionäre oder Inhaberaktien haben; (iv) bargeldintensives Geschäft; (v) die Eigentumsstruktur der juristischen Person oder Rechtsvereinbarung angesichts der Art der Geschäftstätigkeit der juristischen Person oder Rechtsvereinbarung ungewöhnlich oder übermäßig komplex erscheint; oder (vi) der Kunde oder der wirtschaftliche Eigentümer des Kunden ist ein PEP oder ein ausländischer PEP. (b) Risikofaktoren für Produkte, Dienstleistungen, Transaktionen oder Lieferkanäle: (i) anonyme Transaktionen (die Bargeld beinhalten können); oder (ii) häufige Zahlungen von unbekannten oder nicht verbundenen Dritten. (c) Länderrisikofaktoren. Wir verbieten strikt alle Geschäfte, Banküberweisungen und Transaktionen mit Kunden aus Ländern mit hohem Risiko, einschließlich, aber nicht beschränkt auf: (i) Länder oder Gerichtsbarkeiten, bei denen glaubwürdige Quellen wie gegenseitige Evaluierungen oder detaillierte Beurteilungsberichte ergeben haben, dass sie nicht über wirksame AML- und CTF-Systeme verfügen; (ii) von der Financial Action Task Force identifizierte Länder; (iii) Länder oder Gerichtsbarkeiten, die nach glaubwürdigen Quellen ein erhebliches Maß an Korruption oder anderen kriminellen Aktivitäten aufweisen; (iv) Länder oder Gerichtsbarkeiten, die Sanktionen, Embargos oder ähnlichen Maßnahmen unterliegen, beispielsweise von den Vereinten Nationen; oder

(v) Länder, Gerichtsbarkeiten oder geografische Gebiete, von denen glaubwürd ige Quellen berichten, dass sie terroristische Aktivitäten finanzieren oder unters tützen oder die terroristische Organisationen als solche identifiziert haben.

7.3. Das Unternehmen behält sich das Recht vor, für verstärkte Due-Diligence-Maßnahmen I nformationen von unserer unabhängigen Quelle einzuholen. Dazu gehören unter anderem:

(a) Einholung zusätzlicher Informationen über den Kunden (z. B. Beruf, Vermögensu mfang, Eigentums- und Kontrollstruktur, Ruf des Kunden oder wirtschaftlichen Eigent ümers, in öffentlichen Datenbanken, im Internet usw. verfügbare Informationen) und r egelmäßigere Aktualisierung der Identifikationsdaten des Kunden und des wirtschaftlic hen Eigentümers; (b) Einholung zusätzlicher Informationen über die beabsichtigte Art, den Zweck und den Hintergrund der Geschäftsbeziehung und der Transaktionen; (c) E inholung von Informationen über die Geldquelle oder Vermögensquelle des Kunden; (d) Einholung von Informationen über die Gründe für beabsichtigte oder durchgeführte Transaktionen; und/oder (e) verlangen, dass die erste Zahlung über ein Konto im Nam en des Kunden bei einer Bank erfolgt, die ähnlichen CDD-Standards unterliegt.

7.4. Unser EDD beinhaltet:

7.4.1. Erhöhung der Menge der für die Kunden-Due-Diligence eingeholten Informatio nen:

(a) Über die Identität des Kunden oder des wirtschaftlichen Eigentümers oder die Eigentums- und Kontrollstruktur, um sicherzustellen, dass das mit der Bez iehung verbundene Risiko wohlbekannt ist. Dies kann das Einholen und Bew erten von Informationen über den Ruf des Kunden oder des wirtschaftlichen E igentümers sowie die Bewertung etwaiger negativer Vorwürfe gegen den Kun den oder den wirtschaftlichen Eigentümer umfassen. Beispiele hierfür sind: I nformationen über Familienmitglieder und enge Geschäftspartner; Informatio nen über die früheren und gegenwärtigen Geschäftsaktivitäten des Kunden od er wirtschaftlichen Eigentümers; und unerwünschte Medienrecherchen;

(b) Über die beabsichtigte Art der Geschäftsbeziehung, um festzustellen, ob di e Art und der Zweck der Geschäftsbeziehung legitim sind, und um Firmen da bei zu helfen, ein vollständigeres Kundenrisikoprofil zu erhalten. Dazu gehört die Einholung von Informationen über: (i) die Anzahl, Größe und Häufigkeit der Transaktionen, die voraussichtlich über das Konto abgewickelt werden, u m Abweichungen erkennen zu können, die Anlass zu Verdacht geben könnten , und gegebenenfalls Beweise anzufordern; (ii) der Grund, warum der Kunde nach einem bestimmten Produkt oder einer bestimmten Dienstleistung sucht, i nsbesondere wenn unklar ist, warum die Bedürfnisse des Kunden nicht auf an dere Weise oder in einer anderen Gerichtsbarkeit besser erfüllt werden können ; (iii) die Bestimmung der Gelder; (iv) die Art des Geschäfts des Kunden ode r des wirtschaftlichen Eigentümers, um die wahrscheinliche Art der Geschäfts beziehung besser zu verstehen.

7.4.2. Verbesserung der Qualität der für Kunden-Due-Diligence-Zwecke eingeholten I nformationen zur Bestätigung der Identität des Kunden oder des wirtschaftlichen Eige ntümers, unter anderem durch:

(a) Die erste Zahlung muss über ein nachweisbares, auf den Namen des Kund en lautendes Konto bei einer Bank erfolgen; (b) Feststellung, dass es sich bei der Vermögensquelle des Kunden und der in der Geschäftsbeziehung verwend eten Geldquelle nicht um Erträge aus kriminellen Aktivitäten handelt und dass sie mit unserem Wissen über den Kunden und die Art der Geschäftsbeziehung übereinstimmen. Die Quellen der Gelder oder des Vermögens können unter a nderem anhand von Einkommensteuererklärungen, Kopien geprüfter Konten, Gehaltsabrechnungen, öffentlichen Urkunden oder unabhängigen und glaubw ürdigen Medienberichten überprüft werden; (c) Erhöhung der Häufigkeit von Überprüfungen, um sicherzustellen, dass wir weiterhin in der Lage sind, das mit der einzelnen Geschäftsbeziehung verbundene Risiko zu bewältigen, und um bei der Identifizierung von Transaktionen zu helfen, die einer weiteren Üb erprüfung bedürfen, unter anderem durch: (i) Erhöhung der Häufigkeit von Ü berprüfungen der Geschäftsbeziehung, um festzustellen, ob sich das Risikopro fil des Kunden geändert hat und ob das Risiko beherrschbar bleibt; (ii) Einhol en der Zustimmung des leitenden Angestellten/ernannten leitenden Angestellt en zur Aufnahme oder Fortsetzung der Geschäftsbeziehung, um sicherzustelle n, dass sich die Geschäftsleitung des Risikos bewusst ist, dem wir ausgesetzt s ind, und eine fundierte Entscheidung darüber treffen kann, inwieweit sie für di e Bewältigung dieses Risikos gerüstet ist; (iii) Regelmäßigere Überprüfung d er Geschäftsbeziehung, um sicherzustellen, dass alle Änderungen am Risikopr ofil des Kunden erkannt, bewertet und gegebenenfalls darauf reagiert werden; (iv) Durchführung einer häufigeren oder eingehenderen Transaktionsüberwac hung, um ungewöhnliche oder unerwartete Transaktionen zu identifizieren, di e den Verdacht auf Geldwäsche oder Terrorismusfinanzierung begründen kön nten. Dies kann die Feststellung des Bestimmungsortes von Geldern oder die Feststellung des Grundes für bestimmte Transaktionen umfassen; (d) Der Ver antwortliche muss die Genehmigung oder Ablehnung erteilen, mit dem Kunde neinrichtungsprozess fortzufahren, bevor er Geschäfte mit einem Kunden tätig t, der den erweiterten Due-Diligence-Prozess durchlaufen hat.

7.5. Wir wenden EDD-Maßnahmen auf alle Situationen, Kunden oder Transaktionen an, die wir als risikoreich erachten.

7.6. Quelle der Gelder und Quelle des Reichtums

7.6.1. Unter Vermögensquelle versteht man die Herkunft des gesamten Vermögens ei ner Person (d. h. des Gesamtvermögens). 7.6.2. Die Herkunft der Gelder bezieht sich auf die Herkunft der bestimmten Gelder oder anderen Vermögenswerte, die Gegenstan d der Geschäftsbeziehung zwischen einer Person und sind

uns (z.B. die Beträge, die im Rahmen der Geschäftsbeziehung angelegt, einge zahlt oder überwiesen werden).

7.7. Wie die Kennzahlen „Quelle der Mittel“ und „Quelle des Reichtums“ in unseren EDD-Pr ozess integriert werden

7.7.1. Die Vermögensquelle gibt in der Regel die Höhe des Vermögens an, über das d er Kunde voraussichtlich verfügen würde, sowie ein Bild davon, wie die Person dieses Vermögen erworben hat. Auch wenn uns möglicherweise keine spezifischen Informati onen zu Vermögenswerten vorliegen, die nicht bei uns hinterlegt oder von ihr verarbeit et werden, ist es möglicherweise möglich, allgemeine Informationen aus individuellen, kommerziellen Datenbanken oder anderen offenen Quellen zu sammeln. 7.7.2. Infor mationen über die Herkunft der Gelder sollten sich nicht nur darauf beschränken, zu wi ssen, von wem die Gelder möglicherweise überwiesen wurden, sondern auch auf die A ktivität, die die Gelder generiert. Die eingeholten Informationen sollten substanziell se in und die Herkunft oder den Grund für den Erwerb der Gelder belegen.

7.8. Es gehört zu den Grundsätzen des Unternehmens, keine Finanzierung von Dritten anzune hmen. Sollten jedoch solche außergewöhnlichen Umstände eintreten, führen wir eine EDD dur ch, um den letztendlichen wirtschaftlichen Eigentümer zu identifizieren und zu überprüfen, ei nschließlich juristischer Personen, Personengesellschaften, Trusts und anderer Rechtsvereinba rungen.

8. ÜBERPRÜFUNG

8.1. Wir werden die oben genannten Kundeninformationen durch unsere Kundendienst- und Risikomanagementabteilung überprüfen und überprüfen, bevor wir eine Beziehung zu ihnen a ufbauen. Unser CDD-Bereich umfasst unter anderem unsere Privatkunden, Geschäftspartner, Vorstandsmitglieder, Aktionäre und den letztendlichen wirtschaftlichen Eigentümer. Wir führ en folgende CDD-Maßnahmen durch:

(a) die Identität und Informationen des Kunden mithilfe eines unabhängigen Überprüfu ngssystems identifizieren, überprüfen und überprüfen; (b) wenn es in Bezug auf den K unden einen wirtschaftlichen Eigentümer gibt, die Identifizierung und Ergreifung ange messener Maßnahmen zur Überprüfung der Identität des wirtschaftlichen Eigentümers, sodass wir davon überzeugt sind, dass wir wissen, wer der wirtschaftliche Eigentümer i st, einschließlich in dem Fall, dass der Kunde eine juristische Person oder ein Trust ist, Maßnahmen, die es uns ermöglichen, die Eigentums- und Kontrollstruktur der juristisc hen Person oder des Trusts zu verstehen; (c) Einholung von Informationen über den Z weck und die beabsichtigte Art der mit uns bestehenden Geschäftsbeziehung (falls vor handen), es sei denn, der Zweck und die beabsichtigte Art sind offensichtlich; und (d) wenn eine Person vorgibt, im Namen des Kunden zu handeln: (i) Identifizierung der Pe rson und Ergreifen angemessener Maßnahmen zur Überprüfung der Identität der Perso n anhand von Dokumenten, Daten oder Informationen, die von zuverlässigen und unab hängigen Quellen stammen; und (ii) Überprüfung der Befugnis der Person, im Namen des Kunden zu handeln;

(e) Wenn wir die Identitätsüberprüfung als unzureichend erachten oder zusätzliche An gaben benötigen, die für die vom Kunden durchgeführte Transaktion relevant sind, beh alten wir uns das Recht vor, zusätzliche Angaben vom Kunden anzufordern (einschließ lich, aber nicht beschränkt auf

Kontoauszug, Bankkontonachweis, elektronische Geldbörse oder elektronisch er Währungsauszug) und behalten uns das Recht vor, keine Geschäftspartners chaft einzugehen oder keine weitere Transaktion durchzuführen. Wenn der K unde die Bereitstellung der erforderlichen Informationen verweigert oder falsc he/irreführende Informationen bereitstellt, können wir das Kundenkonto sperr en, den Handel oder die Kontoaktivität einschränken, die Geschäftspartnersch aft beenden und/oder der Aufsichtsbehörde Bericht erstatten. Nach zufriedens tellender Überprüfung der Identität des Kunden und der Transaktionsdetails w erden alle für das Konto geltenden Beschränkungen aufgehoben.

8.2. Im Rahmen der Identitätsprüfung fordern wir eine Kopie des Originals und eine farbige S cankopie der Ausweisdokumente an; Wir können auch mehr als ein Ausweisdokument zur Ge genüberprüfung anfordern, wenn wir dies für erforderlich halten.

8.3. Wenn eine elektronische Verifizierung verwendet wird oder ein Kunde zu Identifikations zwecken nicht physisch anwesend war, führen wir eine zusätzliche Verifizierungsprüfung dur ch, um das Risiko von Identitätsbetrug zu minimieren. Diese Prüfung kann wie folgt erfolgen:

(a) verlangen, dass die erste Zahlung über ein auf den Namen des Kunden lautendes K onto bei einem regulierten Kreditinstitut erfolgt; (b) telefonischer Kontakt mit dem Ku nden unter einer verifizierten Privat- oder Geschäftsnummer vor der Kontoeröffnung; (c) Kommunikation mit dem Kunden unter der verifizierten Adresse; (d) die Anforder ung, dass Kopien von Dokumenten von einer geeigneten Person beglaubigt werden.

8.4. Wenn wir nicht in der Lage sind, das vorgeschriebene Identifizierungsverfahren bei einer Person durchz

(a) darf kein Konto für die Person eröffnen; (b) darf keine Geschäftsbeziehung mit der Person eingehen; und (c) sofern mit der Person bereits eine Geschäftsbeziehung besteh t, werden wir die bestehende Geschäftsbeziehung beenden.

9. BERICHT

9.1. Wenn uns nicht innerhalb von 14 Arbeitstagen (2 Arbeitstage, wenn Klausel 4.4(d) und (e) vorliegt) ein zufriedenstellender Nachweis der Identität oder Verifizierung einer Person vor gelegt oder von uns eingeholt wird, übermitteln wir den zuständigen Aufsichtsbehörden einen Bericht über verdächtige Aktivitäten. Wir werden die Transaktion nicht weiter durchführen, es sei denn, die zuständigen Aufsichtsbehörden weisen uns dazu an.

9.2. Für den Fall, dass wir begründeten Verdacht haben, dass der Kunde nicht die Person ist, f ür die er sich ausgibt, werden wir innerhalb von 3 Werktagen, beginnend nach dem Tag, an de m der Umstand eintritt, eine oder mehrere der folgenden Maßnahmen ergreifen:

(i) die erforderlichen Kundenidentifikationsinformationen in Bezug auf den Kunden s ammeln; oder (ii) bestimmte Kundeninformationen, die über den Kunden eingeholt w urden, aus einer zuverlässigen und unabhängigen Quelle überprüfen; um sicherzustelle n, dass hinreichend davon ausgegangen werden kann, dass der Kunde die Person ist, fü r die er sich ausgibt.

9.3. Bei der Festlegung und Einführung geeigneter risikobasierter Systeme und Kontrollen be rücksichtigen wir die Art, Größe und Komplexität des Geschäfts des Kunden sowie dessen Art

ML- und TF-Risiken, denen wir vernünftigerweise ausgesetzt sein könnten, einschließl ich, aber nicht beschränkt auf die folgenden Faktoren:

(a) Kundentypen, einschließlich PEPs; (b) die Art der bereitgestellten ausgewiesenen Dienste; (c) die Art und Weise, wie wir bestimmte Dienstleistungen erbringen, einschl ießlich der Entwicklung neuer Produkte, Geschäftspraktiken und der Nutzung neuer od er sich entwickelnder Technologien; (d) die ausländischen Jurisdiktionen, mit denen w ir Geschäfte machen, einschließlich der von der Financial Action Task Force ermittelte n Hochrisiko-Jurisdiktionen.

9.4. Wenn eines der folgenden Ereignisse eintritt:

(a) verdächtige Transaktion; (b) verdächtige Aktivität; (c) Transaktionen, die von Gel dwäscheunternehmen durchgeführt werden; (d) Transaktionen mit terroristischem Eig entum; (e) Transaktion ohne legitimen Zweck; (f) unser Aufsichtsorgan oder Prüfer h at begründeten Anlass zu der Annahme, dass es sich bei einer Transaktion oder einem Transaktionsversuch oder bei in seinem Besitz befindlichen Informationen um Erträge aus Straftaten handelt oder mit der Finanzierung von Terrorismus zusammenhängt; ode r (g) jede in Klausel 3.2 beschriebene Transaktion; Die Transaktion sollte ausgesetzt werden und nicht ohne die Genehmigung des Beamten durchgeführt werden. Unsere Mitarbeiter an vorderster Front melden jede verdächtige Transaktion oder Aktivität un verzüglich dem Beamten, der dann bei Bedarf innerhalb von zwei Arbeitstagen eine ve rdächtige Aktivität oder verdächtige Transaktionsmeldung an die zuständigen Aufsicht sbehörden übermittelt.

9.5. Wenn verdächtige Anzeichen von Geldwäsche festgestellt werden, sollte die Transaktion ausgesetzt und nicht ohne Genehmigung des Beamten durchgeführt werden. Nach Durchführ ung angemessener Untersuchungen wird der Beamte die Angelegenheit den zuständigen Aufsi chtsbehörden melden, wenn wir der Ansicht sind, dass potenziell schwerwiegende ML- und T F-Risiken bestehen. Für den Fall, dass wir davon ausgehen, dass eine Person zwei oder mehr Transaktionen mit der Absicht durchführt, den in Abschnitt 4.4(b) beschriebenen Betragsschw ellenwert zu umgehen, übermitteln wir den zuständigen Aufsichtsbehörden eine Meldung über verdächtige Transaktionen. Wir werden die folgenden Faktoren berücksichtigen, bevor wir un seren Bericht einreichen:

(a) die Art und Form, in der die Transaktionen durchgeführt wurden; (b) der Betrag der an jeder Transaktion beteiligten Währung; (c) der Gesamtbetrag d er an den Transaktionen beteiligten Währung; (d) der Zeitraum, in dem die T ransaktionen stattgefunden haben; (e) das Zeitintervall zwischen den Transak tionen; (f) die Orte, an denen die Transaktionen eingeleitet oder durchgeführt wurden;

(g) jede Erklärung der betreffenden Person zur Art und Weise oder Form, in der die Tr ansaktionen durchgeführt wurden.

9.6. Verfahren zur Bearbeitung von Meldungen über verdächtige Aktivitäten und Meldungen über verdächtige Transaktionen

9.6.1. Nach Durchführung angemessener Untersuchungen wird der Beamte gegebenen falls erwägen, die Angelegenheit der Regulierungsbehörde zu melden. Alle dem Beam ten und den zuständigen Behörden übermittelten Aufzeichnungen werden vom Beamte n für einen Zeitraum von mindestens sieben Jahren nach Abschluss der Angelegenheit durch die Regulierungsbehörde aufbewahrt. Die Meldung über verdächtige Aktivitäten oder verdächtige Transaktionen muss Folgendes enthalten:

(a) persönliche Daten und Kontaktdaten der Personen oder Organisationen, di e an der verdächtigen Aktivität oder Transaktion beteiligt sind; (b) Einzelheit en der verdächtigen Aktivität oder Transaktion; (c) die beobachteten verdächt igen Aktivitäts- oder Transaktionsindikatoren; und (d) jede Erklärung, die von der Person der Meldung über verdächtige Aktivitäten oder verdächtige Transa ktionen abgegeben wird, wenn sie zu der Transaktion oder Aktivität befragt w ird.

9.6.2. Die Einreichung einer Meldung über verdächtige Aktivitäten oder verdächtige Transaktionen bei den zuständigen Regulierungsbehörden bietet uns eine gesetzliche V erteidigung gegen die Straftat von ML und TF in Bezug auf die in der Meldung offeng elegten Handlungen, vorausgesetzt, dass:

(a) die Meldung verdächtiger Aktivitäten oder verdächtiger Transaktionen erf olgt, bevor wir die offengelegten Handlungen vornehmen, und die Handlunge n oder Transaktionen werden mit Zustimmung der zuständigen Regulierungsb ehörden durchgeführt; oder (b) die Meldung verdächtiger Aktivitäten oder ver dächtiger Transaktionen erfolgt, nachdem wir die offengelegten Handlungen o der Transaktionen durchgeführt haben und die Meldung auf unsere Initiative e rfolgt und sobald dies für uns zumutbar ist.

9.7. Alle getätigten Meldungen werden streng vertraulich behandelt. Bitte beachten Sie jedoc h, dass es Umstände geben kann, in denen wir verpflichtet sind, die Identität einer Person preis zugeben, beispielsweise wenn wir gesetzlich dazu verpflichtet sind und die Anonymität daher nicht gewährleistet werden kann.

9.8. Wir sind uns bewusst, dass es für eine Person, die weiß oder den Verdacht hat, dass eine Offenlegung gegenüber den zuständigen Regulierungsbehörden erfolgt ist, eine Straftat darstel lt, wenn sie einer anderen Person eine Angelegenheit offenlegt, die geeignet ist, eine Untersuc hung zu beeinträchtigen, die im Anschluss an die Offenlegung durchgeführt werden könnte (al lgemein als „Hinweis“ bezeichnet). Das Wissen des Kunden über eine mögliche Meldung ver dächtiger Aktivitäten oder verdächtiger Transaktionen oder Untersuchungen könnte künftige Bemühungen zur Untersuchung des mutmaßlichen ML- und TF-Vorgangs beeinträchtigen. W enn wir daher den Verdacht haben, dass Transaktionen im Zusammenhang mit Geldwäsche un d Terrorismusfinanzierung stehen, berücksichtigen wir bei der Durchführung des CDD-Prozes ses das Risiko eines Hinweises.

Wir stellen sicher, dass sich unsere Mitarbeiter bei der Durchführung von CDD dieser Probleme bewusst sind und dafür sensibel sind.

9.9. Wir wird keine Informationen an Dritte weitergeben Sohn:

(a) dass wir oder unser Aufsichtsorgan oder Prüfer oder eine andere Person einen Verd acht im Zusammenhang mit einer Transaktion oder einem Transaktionsversuch oder ei ner Aktivität oder versuchten Aktivität hegt; oder (b) dass gemäß den geltenden Gesetz en und Vorschriften eine Meldung an die zuständigen Aufsichtsbehörden erfolgt; oder (c) dass Informationen gemäß den geltenden Gesetzen und Vorschriften an die zuständ igen Aufsichtsbehörden weitergegeben werden; oder (d) alle anderen Informationen, a us denen eine Person, der die Informationen offengelegt werden, vernünftigerweise er warten kann, dass sie auf die in den Absätzen (a)−(c) genannten Umstände schließen k ann.

9.10. Klausel 9.9 gilt nicht für eine Offenlegung gegenüber:

(a) ein leitender Angestellter, Mitarbeiter oder Vertreter des Unternehmens, der gemäß diesen geltenden Gesetzen und Vorschriften einen Bericht erstellt oder dazu verpflichte t ist, Informationen zu irgendeinem Zweck im Zusammenhang mit der Erfüllung unser er Pflichten bereitzustellen; oder (b) einen Anwalt, um Rechtsberatung oder -vertretun g im Zusammenhang mit der Offenlegung einzuholen; oder (c) der Vorgesetzte des Un ternehmens; oder (d) eine Strafverfolgungsbehörde oder eine andere Person, die die zu ständigen Regulierungsbehörden gemäß diesen geltenden Gesetzen und Vorschriften u nterstützt.

9.11. Zu den Aufgaben unseres Beamten gehören unter anderem:

(a) Überprüfen Sie alle internen Berichte über verdächtige Transaktionen und Ausnah meberichte und stellen Sie anhand aller verfügbaren Informationen fest, ob es notwend ig ist, bei den zuständigen Aufsichtsbehörden einen Bericht über verdächtige Aktivität en oder verdächtige Transaktionen einzureichen. (b) alle Aufzeichnungen im Zusamm enhang mit solchen internen Überprüfungen aufbewahren; (c) Anleitung des Personals , wie man „Hinweise“ vermeidet, wenn eine Meldung über verdächtige Aktivitäten ode r verdächtige Transaktionen eingereicht wird; (d) Anwendbare Gesetze und Vorschrift en als Hauptansprechpartner für die zuständigen Regulierungsbehörden, Strafverfolgun gsbehörden und alle anderen zuständigen Behörden in Bezug auf die Prävention und E rkennung, Untersuchung oder Einhaltung von Geldwäsche und Terrorismusfinanzierun g.

10. LAUFENDE CDD- UND TRANSAKTIONSÜBERWACHUNG

10.1. Wir werden eine kontinuierliche Überwachung durch laufende CDD- und Transaktionsü berwachung durchführen, um die Einhaltung der AML- und CTF-Systeme sicherzustellen. Wi r überprüfen die vorhandenen CDD-Aufzeichnungen bei jedem auslösenden Ereignis und unte rhalten angemessene Systeme zur Überwachung von Transaktionen gemäß dem gewählten risi kobasierten Ansatz. Der Umfang der Überwachung muss proportional zum ML- und TF-Risik oprofil eines Kunden sein.

10.2. Laufende CDD

10.2.1. Wir überwachen kontinuierlich die Aktivitäten unserer Kunden durch:

(a) von Zeit zu Zeit Überprüfung der Dokumente, Daten und Informationen in Bezug auf den Kunden, die zur Erfüllung der CDD-Anforderungen eingeholt wurden, um sicherzustellen, dass sie aktuell und relevant sind; (b) Durchführung einer angemessenen Prüfung der für den Kunden durchgeführten Transaktionen, um sicherzustellen, dass diese mit unserem Wissen über den Kunden und dessen Geschäft, Risikoprofil und Finanzierungsquelle übereinstimmen; und (c) Identifizierung von Transaktionen, die komplex sind, einen ungewöhnlich großen Umfang haben oder ein ungewöhnliches Muster aufweisen oder die keinen erkennbaren wirtschaftlichen oder rechtmäßigen Zweck haben und die auf Geldwäsche und Terrorismusfinanzierung hinweisen können.

10.2.2. Alle Kunden, die Folgendes aufweisen: (a) hohe ML- und TF-Risiken, sollten alle 6 Monate einer Überprüfung unterzogen werden; (b) mittlere GW- und TF-Risiken sollten einmal jährlich einer Überprüfung unterzogen werden; (c) geringe GW- und TF-Risiken sollten alle zwei Jahre einer Überprüfung unterzogen werden;

oder häufigere Überprüfungen, wenn wir dies für notwendig erachten, um sicherzustellen, dass die gespeicherten CDD-Informationen mit unserem Wissen über den Kunden, das Geschäft des Kunden, die Geldquelle und das Risikoprofil übereinstimmen.

10.2.3. Alle Kunden, die als Hochrisikopatienten eingestuft wurden, werden einer vollständigen Überprüfung unterzogen. Hierzu ist Folgendes festzulegen:

Erneute Adressbestätigung

Erneute Bestätigung der Unternehmensstruktur (falls zutreffend)

Erneute Bestätigung der Herkunft der Mittel und des Vermögens

Screening auf negative Nachrichten

Vollständige Überprüfung des Transaktionsprofils, einschließlich der angeforderten neuen Produkte

10.3. Transaktionsüberwachung

10.3.1. Wir unterhalten angemessene Systeme zur Überwachung und Überprüfung aller durchgeführten Transaktionen auf der Grundlage eines risikobasierten Ansatzes und prüfen und überprüfen anhand der folgenden Faktoren, ob die Transaktionen normal sind:

(a) die Größe und Komplexität seines Geschäfts; (b) die ML- und TF-Risiken, die sich aus seiner Geschäftstätigkeit ergeben; (c) die Art seiner Systeme und Kontrollen; (d) die Überwachungsverfahren, die bereits zur Erfüllung anderer Geschäftsanforderungen vorhanden sind; und (e) die Art der bereitgestellten Produkte und Dienstleistungen (einschließlich der Liefer- oder Kommunikationsmittel).

10.3.2. Wir überprüfen regelmäßig die Angemessenheit und Wirksamkeit unserer Transaktionsüberwachungssysteme und -prozesse, einschließlich Parameter und Schwellenwerte

angenommen. Die angenommenen Parameter und Schwellenwerte umfassen die folgenden Faktoren:

(a) die Art und Art der Transaktionen (z. B. ungewöhnliche Größe oder Häufigkeit); (b) die Art einer Reihe von Transaktionen (z. B. Strukturierung einer einzelnen Transaktion in mehrere Bareinlagen); (c) die Gegenparteien von Transaktionen; (d) der geografische Ursprung/Zielort einer Zahlung oder Quittung; (e) die normale Kontoaktivität oder der normale Kontoumsatz des Kunden; (f) das Verhalten des Kunden – plötzliche und/oder erhebliche Änderungen der Transaktionsaktivität nach Wert, Volumen oder Art, wie z. B. Änderung des Begünstigten oder Bestimmungsortes; (g) verbundene Kundenbeziehungen – Identifizierung gemeinsamer Begünstigter und Überweiser unter scheinbar nicht verbundenen Konten oder Kunden.

11. AUFZEICHNUNG

11.1. Aufzeichnungen aller Originale und Kopien von Dokumenten zur Identitätsprüfung, Transaktionsaufzeichnungen, CDD-Informationen, ML- und TF-Berichte, die an den Beamten übermittelt werden, alle im Zusammenhang mit der Meldung über verdächtige Aktivitäten, der Meldung über verdächtige Transaktionen eingereichten Dokumente, das Personal, das die Meldung über verdächtige Transaktionen bearbeitet, die Ergebnisse der Meldung über verdächtige Transaktionen und andere im Rahmen des Beamten erforderliche Dokumente werden für mindestens 7 Jahre nach dem Ende der Geschäftsbeziehung mit Kunden vertraulich zusammengestellt und organisiert.

11.2. Die Aufzeichnungspflichten für jeden Kunden lauten wie folgt:

(A) Wir müssen das Original oder eine Kopie von (i) den Dokumenten und einer Aufzeichnung der Daten und Informationen aufbewahren, die wir im Zuge der Identifizierung und Überprüfung der Identität des Kunden erhalten haben; wirtschaftlicher Eigentümer des Kunden; und die Person, die vorgibt, im Namen des Kunden zu handeln; und (ii) die Dateien im Zusammenhang mit der Geschäftsbeziehung des Kunden und der Geschäftskorrespondenz mit dem Kunden und etwaigen wirtschaftlichen Eigentümern des Kunden; Und

(b) Die in Absatz (a) oben genannten Dokumente und Aufzeichnungen sind während der gesamten Dauer der Geschäftsbeziehung mit dem Kunden und mindestens sieben Jahre lang ab dem Datum der Beendigung der Geschäftsbeziehung aufzubewahren.

11.3. Die Anforderungen an die Aufbewahrung von Aufzeichnungen in Bezug auf jede Transaktion lauten wie folgt: (a) Wir bewahren das Original oder eine Kopie der Dokumente sowie eine Aufzeichnung der im Zusammenhang mit der Transaktion erhaltenen Daten und Informationen auf, einschließlich, aber nicht beschränkt auf Folgendes: (i) Art der Transaktion; (ii) der Betrag der Transaktion und die Währung, auf die sie lautete; (iii) das Datum, an dem die Transaktion durchgeführt wurde;

(iv) Name, Adresse und Beruf, Geschäft oder Haupttätigkeit, je nach Fall, jeder Person: (aa) Durchführung der Transaktion; und (ab) für wen oder zu dessen ultimative m Vorteil die Transaktion durchgeführt wird, wenn wir berechtigten Grund zu der Ann ahme haben, dass die Person die Transaktion im Namen einer anderen Person durchfüh rt; (v) die Art und Identifikationsnummer aller Konten/Dienste bei uns, die an der Tra nsaktion beteiligt waren; (vi) wenn es sich bei der Transaktion um ein anderes handelb ares Instrument als eine Währung handelt: (aa) der Aussteller des Instruments; (bb) de r Name der Institution, auf die es sich bezieht; (cc) der Name des Zahlungsempfängers (falls vorhanden); (dd) Betrag und Datum des Instruments; und (ee) die Nummer (falls vorhanden) des Instruments und Einzelheiten zu etwaigen Vermerken, die auf dem Inst rument erscheinen; (vii) Name und Adresse des Unternehmens sowie aller leitenden A ngestellten, Mitarbeiter oder Vertreter des Unternehmens, die die relevanten Aufzeichn ungen oder einen Teil der Aufzeichnungen erstellt haben; (viii) alle anderen Informati onen im Zusammenhang mit dieser Transaktion. (b) Aufzeichnungen, die gemäß Unte rabsatz (a) aufzubewahren sind, müssen ab dem Datum des Abschlusses der Transaktio n mindestens sieben Jahre lang aufbewahrt werden, unabhängig davon, ob die Geschäft sbeziehung in diesem Zeitraum endet.

12. AML- UND CTF-SCREENING-VERFAHREN

12.1. Kunden werden anhand von Sanktionslisten, politisch exponierten Personen, behördlich er Durchsetzung, Strafverfolgung, Geldwäsche, Terrorismusfinanzierung und negativen Medie nberichten überprüft, die vom World-Check One-Überprüfungssystem von Refinitiv Limited b ereitgestellt werden. Kunden werden zur laufenden Überwachungsliste von World-Check One hinzugefügt, wobei ihre Daten alle 12 Stunden automatisch vom System durchsucht werden. Wir erhalten eine Benachrichtigung, sobald es positive Übereinstimmungen gibt.

12.2. Wir screenen:

(a) Kunden und etwaige wirtschaftliche Eigentümer der Kunden anhand der aktuellen Datenbank zum Zeitpunkt der Einrichtung der Beziehung; (b) Kunden und alle wirtsc haftlichen Eigentümer der Kunden so schnell wie möglich gegen alle neuen und alle ak tualisierten Bezeichnungen in der Datenbank; und (c) alle relevanten Parteien einer gre nzüberschreitenden Überweisung mit der aktuellen Datenbank vor der Ausführung der Überweisung.

12.3. Bei Verdacht auf Terrorismusfinanzierung, Proliferationsfinanzierung und Verstöße geg en Sanktionen werden wir den zuständigen Aufsichtsbehörden eine Meldung über verdächtige Aktivitäten oder verdächtige Transaktionen vorlegen. Wir werden alle eingefrorenen Vermög enswerte oder ergriffenen Maßnahmen melden

Einhaltung der Finanzsanktionsanforderungen durch Einreichung einer Meldung über verdächtige Aktivitäten oder verdächtige Transaktionen bei den zuständigen Aufsichts behörden.

13. AML- UND CTF-PRÜFFUNKTION

13.1. Der Beauftragte und unsere Compliance-Abteilung führen jährlich eine interne Prüfung unserer AML- und CTF-Richtlinien durch, um sicherzustellen, dass unsere AML- und CTF-Ri chtlinien aktualisiert werden. Wir sind uns unserer gesetzlichen Verpflichtung zur Einhaltung der geltenden Gesetze und Vorschriften bewusst und werden unsere AML- und CTF-Richtlini e mindestens einmal jährlich aktualisieren und überprüfen.

13.2. Wir werden regelmäßig ML- und TF-Risiken identifizieren und bewerten, die in Bezug auf Folgendes

(a) die Art und das Ausmaß des Geldwäsche- und Terrorismusfinanzierungsrisikos, mit dem wir im Rahmen unserer Geschäftstätigkeit vernünftigerweise rechnen können; (b) die Art, Größe und Komplexität unseres Geschäfts; (c) Entwicklung neuer Produkte u nd neuer Geschäftspraktiken, einschließlich neuer Bereitstellungsmechanismen; und (d) Einsatz neuer oder sich entwickelnder Technologien sowohl für neue als auch für ber eits bestehende Produkte.

14. TRAININGSPROGRAMM

14.1. Alle relevanten Mitarbeiter im Unternehmen erhalten die entsprechenden Richtlinien- u nd Wissensschulungen, die in dieser AML- und CTF-Richtlinie bereitgestellt werden. Darübe r hinaus werden alle relevanten Mitarbeiter im Unternehmen über ihre Stellenbeschreibungen i nformiert und über ihre Verantwortlichkeiten in Bezug auf Geldwäsche und Finanzierung terr oristischer Transaktionen geschult. Sie werden darin angeleitet, Transaktionen zu erkennen u nd abzuwickeln, bei denen es sich möglicherweise um Geldwäsche und Terrorismusfinanzieru ng handelt.

14.2. Umfang der Ausbildung

14.2.1. Das Personal wird auf Folgendes aufmerksam gemacht:

(a) unsere gesetzlichen Verpflichtungen und deren gesetzliche Verpflichtunge n sowie die möglichen Konsequenzen, wenn wir verdächtige Transaktionen g emäß den geltenden Gesetzen und Vorschriften sowie der Verordnung nicht m elden; (b) alle anderen gesetzlichen und behördlichen Verpflichtungen, die un s gemäß den geltenden Gesetzen und Vorschriften und der Verordnung betreff en, sowie die möglichen Folgen von Verstößen gegen diese Verpflichtungen; (c) unsere Richtlinien und Verfahren in Bezug auf AML und CTF, einschließl ich verdächtiger Aktivitäten sowie der Identifizierung und Meldung von Trans aktionen; (d) alle neuen und aufkommenden Techniken, Methoden und Trend s im Bereich Geldwäsche und Terrorismusfinanzierung, sofern diese Informat ionen von den Mitarbeitern zur Wahrnehmung ihrer jeweiligen Aufgaben in B ezug auf Geldwäsche und Terrorismusfinanzierung benötigt werden; (e) Eska lationsverfahren, d. h. was zu tun ist, sobald ein GW- und TF-Risiko festgestel lt wird; (f) welche Rolle der Mitarbeiter bei unseren Compliance-Bemühunge n spielt und wie er diese umsetzt; (g) Richtlinie zur Führung von Aufzeichnu ngen und zur Aufbewahrung von Aufzeichnungen; Und

(h) disziplinarische Konsequenzen (zivil- und strafrechtlich) bei Nichteinhaltu ng der geltenden Gesetze und Vorschriften.

14.2.2. Durch gezielte Schulungen für geeignete Mitarbeiter oder Mitarbeitergruppen können das Unternehmen und die Geschäftsleitung ihre AML- und CTF-Systeme effek tiv implementieren. Die folgenden Ausbildungsbereiche können mit Sicherheit geeign et sein

Mitarbeitergruppen: (a) Alle neuen Mitarbeiter (unabhängig vom Dienstalter) (i) eine Einführung in den Hintergrund von ML und TF und die Bedeutung vo n AML und CTF für uns; und (ii) die Notwendigkeit und Verpflichtung, verdä chtige Transaktionen zu identifizieren und dem Beamten zu melden, sowie de r Straftatbestand des „Tipping-off". (b) Mitarbeiter an vorderster Front (d. h. Mitarbeiter, die sich direkt mit Kunden befassen) (i) die Bedeutung ihrer Roll e in der AML- und CTF-Strategie des Unternehmens als erste Anlaufstelle für potenzielle Geldwäscher und an TF beteiligte Personen; (ii) die Richtlinien u nd Verfahren des Unternehmens in Bezug auf CDD- und Aufzeichnungsanfor derungen, die für ihre beruflichen Verantwortlichkeiten relevant sind; (iii) An leitungen oder Tipps zur Identifizierung ungewöhnlicher Aktivitäten unter ver schiedenen Umständen, die Anlass zu Verdacht geben könnten; und (iv) die re levanten Richtlinien und Verfahren für die Meldung ungewöhnlicher Aktivität en, einschließlich der Meldelinie und der Umstände, unter denen möglicherwe ise besondere Wachsamkeit erforderlich ist.

(c) Back-Office-Mitarbeiter (i) angemessene Schulung zur Kundenüberprüfun g und den relevanten Verarbeitungsverfahren; und (ii) Möglichkeiten zur Erke nnung ungewöhnlicher Aktivitäten, einschließlich abnormaler Abrechnungen, Zahlungen oder Lieferanweisungen.

(d) Führungskräfte (einschließlich interner Revisionsmitarbeiter) (i) weiterfüh rende Schulungen, die alle Aspekte des AML- und CTF-Regimes abdecken; (ii) spezifische Schulung in den für uns geltenden AML- und CTF-Anforderun gen; und (iii) spezifische Schulungen in Bezug auf ihre Verantwortung für die Überwachung oder Führung von Mitarbeitern, die Prüfung des Systems und di e Durchführung von Stichprobenkontrollen sowie die Meldung verdächtiger T ransaktionen an die zuständigen Aufsichtsbehörden.

(e) Offizier

(i) spezifische Schulung in Bezug auf die Verantwortlichkeiten des Bea mten für die Beurteilung der ihm vorgelegten verdächtigen Transaktions meldungen und die Meldung verdächtiger Transaktionen an die zuständi gen Aufsichtsbehörden;

(ii) Schulung, um allgemein über die AML- und CTF-Anforderungen/Entwicklungen auf dem Laufenden zu bleiben; (iii) Berichte über verdächtige Aktivitäten von Firmenmitarbeitern erhalten; und (iv) die erforderlichen Überprüfungen/Besprechungen zur Bekämpfung der Geldwäsche mit den entsprechenden Mitarbeitern zu koordinieren.

14.3. Wir überwachen die Wirksamkeit des Trainings. Dies kann erreicht werden durch:

(a) Prüfung des Verständnisses der Mitarbeiter unserer Richtlinien und Verfahren zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung, des Verständnisses ihrer gesetzlichen und behördlichen Verpflichtungen sowie ihrer Fähigkeit, verdächtige Transaktionen zu erkennen; (b) Überwachung der Einhaltung unserer AML- und CTF-Systeme durch das Personal sowie der Qualität und Quantität interner Berichte, damit weiterer Schulungsbedarf ermittelt und geeignete Maßnahmen ergriffen werden können; und (c) Überwachung der Anwesenheit und Nachverfolgung bei Mitarbeitern, die eine solche Schulung ohne triftigen Grund versäumen.

14.4. Wir führen mindestens einmal jährlich AML-Schulungen, Workshops und Beurteilungen für alle relevanten Mitarbeiter durch.

14.5. Wir werden unsere Mitarbeiter, die angemessen geschult wurden, beobachten und dokumentieren, wann sie geschult werden oder zuletzt geschult werden, und ihnen anschließend zusätzliche, notwendige und angemessene Schulungen anbieten.

15. SPRACHE UND ÄNDERUNGEN

15.1. Die offizielle Sprache dieser AML- und CTF-Richtlinie ist Englisch. Das Unternehmen kann diese AML- und CTF-Richtlinie nur zu Informationszwecken in anderen Sprachen zur Verfügung stellen. Im Falle von Widersprüchen oder Unstimmigkeiten zwischen der englischen Version dieser AML- und CTF-Richtlinie und einer anderen Sprachversion ist die englische Version maßgebend.

15.2. Der Kunde erkennt an, dass sich das Unternehmen das Recht vorbehält, diese AML- und CTF-Richtlinie jederzeit und ohne vorherige Ankündigung an den Kunden zu ändern oder zu aktualisieren. Die Änderungen der AML- und CTF-Richtlinie treten sofort in Kraft und sind für den Kunden mit der Veröffentlichung der AML- und CTF-Richtlinie auf der Website des Unternehmens rechtsverbindlich. Der Kunde verpflichtet sich, diese AML- und CTF-Richtlinie regelmäßig auf der Website des Unternehmens zu überprüfen.

(Der Rest dieser Seite wurde absichtlich leer gelassen.)