RICHTLINIEN ZUR BEKÄMPFUNG VON GELDWÄSCHE UND TERRORISMUSFINANZIERUNG

EINLEITUNG

Der Zweck dieser Richtlinien zur Bekämpfung von Geldwäsche (AML), Terrorismusfinanzierung (CFT) und Sanktionen ist es, sicherzustellen, dass **UAB Criptomy** (Unternehmen) über interne Richtlinien verfügt, um die Nutzung seines Geschäfts für Geldwäsche und Terrorismusfinanzierung zu verhindern, sowie über interne Richtlinien zur Umsetzung internationaler Sanktionen.

Diese Richtlinien wurden verabschiedet, um sicherzustellen, dass das Unternehmen die Regeln und Vorschriften des Gesetzes der Republik Litauen zur Verhinderung von Geldwäsche und Terrorismusfinanzierung (Gesetz) und anderer anwendbarer Gesetze einhält, darunter die folgenden:

- Technische Anforderungen für den Kundenidentifizierungsprozess für die Fernidentifizierungsauthentifizierung über elektronische Geräte für die direkte Videoübertragung, genehmigt vom Direktor des Dienstes für die Untersuchung von Finanzkriminalität des Innenministeriums der Republik Litauen am 30. November 2016 durch den Beschluss Nr. V-314 "Für die technischen Anforderungen für den Kundenidentifizierungsprozess für die Fernidentifizierungsauthentifizierung über elektronische Geräte für die direkte Videoübertragung" (im Folgenden - Technische Anforderungen).[1]

- Beschluss Nr. V-240 vom 5. Dezember 2014 des Direktors des Dienstes für die Untersuchung von Finanzkriminalität des Innenministeriums der Republik Litauen "Über die Genehmigung der Liste der Kriterien für die Identifizierung von Geldwäsche und verdächtigen oder ungewöhnlichen monetären Operationen oder Transaktionen".[2]

- Beschluss Nr. V-5 vom 5. Januar 2020 des Direktors des Dienstes für die Untersuchung von Finanzkriminalität des Innenministeriums der Republik Litauen "Über die Genehmigung von Richtlinien für die Betreiber von Depotbanken für virtuelle Währungen und Betreiber von virtuellen Währungsbörsen zur Verhinderung von Geldwäsche und/oder Terrorismusfinanzierung".[3]

- Beschluss Nr. V-273 vom 20. Oktober 2016 des Direktors des Dienstes für die Untersuchung von Finanzkriminalität des Innenministeriums der Republik Litauen "Über die Genehmigung von Leitlinien für die Überwachung von Finanzkriminalität zur Umsetzung internationaler Finanzsanktionen im Bereich der Vorschriften des Innenministeriums der Republik Litauen".[4]

- des Innenministers der Republik Litauen 2017 Oktober 16 durch die Verordnung Nr. 1V-701 "Über die Aussetzung verdächtiger Geldtransaktionen oder Transaktionen und die Übermittlung von Informationen über verdächtige Geldtransaktionen oder Transaktionen an den Ermittlungsdienst für Finanzkriminalität gemäß der Verfahrensbeschreibung des Innenministeriums der Republik Litauen und Informationen über Bargeldtransaktionen oder Transaktionen in Höhe von 15.000 Euro oder die Übermittlung des entsprechenden Betrags in ausländischer Währung

[1] https://www.e-tar.lt/portal/lt/legalAct/e45f4270b70011e6aae49c0b9525cbbb/asr
[2] https://www.e-tar.lt/portal/lt/legalAct/a664b2107ecd11e4bc68a1493830b8b9
[3] https://www.e-tar.lt/portal/lt/legalAct/570a231035e011ea829bc2bea81c1194
[4] https://www.e-tar.lt/portal/lt/legalAct/01d5d4e0974411e69ad4c8713b612d0f

Währung an den Ermittlungsdienst für Finanzkriminalität unter Genehmigung der Verfahrensbeschreibung des Innenministeriums der Republik Litauen "[5]

- Direktor des Financial Crime Investigation Service 2015 Mai 21 durch Verfügung Nr. V-129 "Über die Genehmigung von Informationsformularen, Einreichungsschemata und Empfehlungen für die Vervollständigung von Informationen, die gemäß den Anforderungen des Gesetzes zur Verhinderung von Geldwäsche und Terrorismusfinanzierung der Republik Litauen bereitgestellt werden"[6]

Diese Richtlinien werden vom Vorstand mindestens einmal jährlich überprüft. Der Vorschlag für eine Überprüfung und die Überprüfung dieser Richtlinien kann auf Beschluss des Geldwäschebeauftragten (MLRO) des Unternehmens oder des Beauftragten für interne Kontrolle häufiger angesetzt werden.

Diese Richtlinien werden durch den Beschluss des Vorstands der Gesellschaft angenommen und genehmigt.

DEFINITIONEN

Wirtschaftlicher Eigentümer ist eine natürliche Person, die unter Ausnutzung ihres Einflusses eine Transaktion, eine Handlung, eine Maßnahme, einen Vorgang oder einen Schritt vornimmt oder in anderer Weise Kontrolle über eine Transaktion, eine Handlung, eine Maßnahme, einen Vorgang oder einen Schritt oder über eine andere Person ausübt und in deren Interesse oder zu deren Gunsten oder auf deren Rechnung eine Transaktion oder eine Handlung, eine Maßnahme, ein Vorgang oder ein Schritt vorgenommen wird. Im Falle einer juristischen Person ist der wirtschaftliche Eigentümer eine natürliche Person, deren direkte oder indirekte Beteiligung oder die Summe aller direkten und indirekten Beteiligungen an der juristischen Person 25 Prozent übersteigt, einschließlich Beteiligungen in Form von Aktien oder anderen Formen von Inhabern.

Geschäftsbeziehung bezeichnet eine Beziehung, die durch den Abschluss eines langfristigen Vertrages durch das Unternehmen im Rahmen einer wirtschaftlichen oder beruflichen Tätigkeit zum Zwecke der Erbringung einer Dienstleistung oder deren Vertrieb auf andere Weise begründet wird oder die nicht auf einem langfristigen Vertrag beruht, bei der jedoch zum Zeitpunkt der Kontaktaufnahme vernünftigerweise mit einer gewissen Dauer gerechnet werden konnte und bei der das Unternehmen im Rahmen der Erbringung einer Dienstleistung wiederholt einzelne Transaktionen im Rahmen einer wirtschaftlichen oder beruflichen Tätigkeit vornimmt.

Unternehmen ist eine juristische Person mit den folgenden Daten:

- Name des Unternehmens: UAB Criptomy;
- Registrierungsland: Litauen;
- Registrierungsnummer: 306127858;
- Adresse: Vilnius, Eišiškių Sodų 18-oji g. 11;
- E-Mail: info@criptomy.exchange, contact@criptomy.exchange

Virtuelle Währungs-Wallet der Depotbank bezeichnet eine oder mehrere virtuelle Währungsadressen, die mit dem öffentlichen Schlüssel[7] erstellt wurden, um virtuelle Währungen zu speichern und zu verwalten, die dem Unternehmen anvertraut wurden, aber sein Eigentum bleiben.

Virtuelle Währungs-Wallet der Depotbank bezeichnet eine oder mehrere virtuelle Währungsadressen, die mit dem öffentlichen Schlüssel[7] erstellt wurden, um virtuelle Währungen zu speichern und zu verwalten, die dem Unternehmen anvertraut wurden, aber sein Eigentum bleiben.

Kunde bedeutet eine natürliche oder juristische Person, die eine Geschäftsbeziehung mit dem Unternehmen unterhält.

Mitarbeiter bezeichnet den Mitarbeiter des Unternehmens und jede andere Person, die an der Anwendung dieser Richtlinien im Unternehmen beteiligt ist.

Richtlinien - dieses Dokument einschließlich aller Anhänge wie oben angegeben. Die Richtlinien beinhalten unter anderem das interne Kontrollverfahren des Unternehmens in Bezug auf die Richtlinien und die Risikobewertungspolitik des Unternehmens in Bezug auf den risikobasierten Ansatz für ML/TF-Risiken.

Vorstand bezeichnet den Vorstand des Unternehmens. Wenn das Unternehmen keinen Vorstand hat, gilt der Geschäftsführer des Unternehmens als Vorstandsmitglied und er oder sie ist für die Aufgaben des Vorstands im Rahmen der Richtlinien verantwortlich.

MLRO bedeutet Money Laundering Reporting Officer (Geldwäsche-Meldebeauftragter), der bei der Gesellschaft als Verantwortlicher für die Entgegennahme interner Meldungen und die Erstellung von Berichten an den Financial Crime Investigation Service (FCIS) sowie für andere Aufgaben, wie oben beschrieben, ernannt wurde.

Monetäre Operation bedeutet jede Zahlung, Überweisung oder Entgegennahme von Geld.

Unter Geldwäsche (ML) versteht man die Verschleierung der Herkunft illegaler Gelder durch ihre Einführung in das legale Wirtschaftssystem und scheinbar legitime Transaktionen. Es gibt drei anerkannte Stufen im Geldwäscheprozess:

- Platzierung, bei der die Erträge aus Straftaten in das Finanzsystem eingebracht werden;
- Layering, d.h. die Umwandlung von Erträgen aus Straftaten in eine andere Form und die Schaffung komplexer Schichten von Finanztransaktionen, um den Prüfpfad sowie die Herkunft und das Eigentum der Gelder zu verschleiern;
- die Integration, bei der die gewaschenen Erlöse wieder in die Wirtschaft fließen, um den Eindruck von Legitimität zu erwecken.

Gelegentliches Geschäft bezeichnet die Transaktion, die das Unternehmen im Rahmen seiner wirtschaftlichen oder beruflichen Tätigkeit zum Zwecke der Erbringung einer Dienstleistung oder des Verkaufs von Waren oder deren Vertrieb auf andere Weise an den Kunden außerhalb einer bestehenden Geschäftsbeziehung durchführt.

PEP bezeichnet eine natürliche Person, die herausragende öffentliche Funktionen ausübt oder ausgeübt hat und in Bezug auf die entsprechende Risiken bestehen.

Sanktionen sind ein wesentliches Instrument der Außenpolitik, um die Aufrechterhaltung oder Wiederherstellung des Friedens, der internationalen Sicherheit, der Demokratie und der Rechtsstaatlichkeit zu unterstützen.

---

[5] https://e-tar.lt/portal/lt/legalAct/143ad320b24011e7afdadfc0e4460de4

[6] https://www.e-tar.lt/portal/lt/legalAct/e1f42fa0006d11e588da8908dfa91cac

[7] **Öffentlicher Schlüssel** ist ein Code aus Buchstaben, Zahlen und/oder Symbolen, der dazu dient, den Kunden zu identifizieren und die Adresse der virtuellen Währung des Kunden zu generieren.

Rechte und des Völkerrechts oder zur Erreichung anderer Ziele der Charta der Vereinten Nationen oder der Gemeinsamen Außen- und Sicherheitspolitik der Europäischen Union. Die Sanktionen umfassen:

- internationale Sanktionen, die in Bezug auf einen Staat, ein Gebiet, eine Gebietseinheit, ein Regime, eine Organisation, eine Vereinigung, eine Gruppe oder eine Person durch eine Resolution des Sicherheitsrates der Vereinten Nationen, einen Beschluss des Rates der Europäischen Union oder andere Rechtsvorschriften, die Litauen Verpflichtungen auferlegen, verhängt werden;
- Sanktionen der Regierung der Republik Litauen, die ein Instrument der Außenpolitik sind und die zusätzlich zu den im vorigen Abschnitt genannten Zielen verhängt werden können, um die Sicherheit oder die Interessen Litauens zu schützen.

Internationale Sanktionen können die Einreise eines Subjekts einer internationalen Sanktion in den Staat verbieten, den internationalen Handel und internationale Transaktionen einschränken und andere Verbote oder Verpflichtungen auferlegen.

Gegenstand von Sanktionen ist jede natürliche oder juristische Person, Organisation oder Einrichtung, die in dem Rechtsakt, mit dem Sanktionen verhängt oder umgesetzt werden, benannt ist und auf die die Sanktionen Anwendung finden.

Terrorismusfinanzierung (TF) bedeutet die Finanzierung und Unterstützung eines terroristischen Akts und dessen Beauftragung sowie die Finanzierung und Unterstützung von Reisen zum Zwecke des Terrorismus im Sinne der geltenden Gesetzgebung.

Drittland bedeutet einen Staat, der nicht Mitglied des Europäischen Wirtschaftsraums (EWR) ist.

Virtuelle Währung ist ein in digitaler Form dargestellter Wert, der digital übertragbar, aufbewahrbar oder handelbar ist und den natürliche oder juristische Personen als Zahlungsmittel akzeptieren, der aber kein gesetzliches Zahlungsmittel eines Landes oder ein Fonds im Sinne von Artikel 4 Absatz 25 der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU sowie der Verordnung (EU) Nr. 1093/2010 und zur Aufhebung der Richtlinie 2007/64/EG (ABl. L 337 vom 23.12.2015, S. 35-127) oder einen Zahlungsvorgang für die Zwecke von Artikel 3 Buchstaben k und l der gleichen Richtlinie.

Die Adresse der virtuellen Währung ist eine Adresse bzw. ein Konto, das aus Buchstaben, Zahlen und/oder Symbolen in der Blockchain generiert wird und über das die Blockchain dem Eigentümer oder Empfänger die virtuelle Währung zuweist.

GRUNDSÄTZE FÜR STRUKTUR UND MANAGEMENT DES UNTERNEHMENS

Die Organisationsstruktur der Gesellschaft muss ihrer Größe und der Art, dem Umfang und dem Komplexitätsgrad ihrer Aktivitäten und erbrachten Dienstleistungen, einschließlich der Risikobereitschaft und der damit verbundenen Risiken, entsprechen und nach dem Prinzip der **drei Verteidigungslinien** aufgebaut sein**.** Die Organisationsstruktur des Unternehmens muss dem vollständigen Verständnis der potenziellen Risiken und deren Management entsprechen. Die Berichts- und Unterstellungsketten des Unternehmens müssen so gewährleistet sein, dass alle Mitarbeiter ihren Platz in der Organisationsstruktur kennen und ihre Arbeitsaufgaben kennen.

Der Vorstand

Der Vorstand ist Träger der Kultur der Einhaltung der Anforderungen zur Verhinderung von Geldwäsche und Terrorismusfinanzierung. Er stellt sicher, dass die Vorstandsmitglieder und Mitarbeiter des Unternehmens in einem Umfeld agieren, in dem sie sich der Anforderungen zur Verhinderung von Geldwäsche und Terrorismusfinanzierung und der damit verbundenen Verpflichtungen voll bewusst sind und die entsprechenden Risikoerwägungen in angemessenem Umfang in den Entscheidungsprozessen des Unternehmens berücksichtigt werden.

Die Vorstandsmitglieder tragen die letztendliche Verantwortung für die Maßnahmen, die getroffen werden, um die Nutzung der Dienste des Unternehmens für Geldwäsche oder Terrorismusfinanzierung zu verhindern. Sie üben die Aufsicht aus und sind rechenschaftspflichtig für:

- Einrichtung und Pflege von AML[8] Prozessen, Verfahren, Risiko- und Kontrollprozessen;
- die Annahme dieser Richtlinien und anderer interner Richtlinien und Anleitungen;
- die Festlegung der Richtlinien des Unternehmens für AML-Maßnahmen;
- die Ernennung eines MLRO und die Sicherstellung, dass der MLRO über die erforderlichen Befugnisse, Ressourcen und Fachkenntnisse verfügt, um seine Aufgabe zu erfüllen;
- Bereitstellung ausreichender Ressourcen, um die wirksame Umsetzung der Leitlinien und anderer damit verbundener Dokumente zu gewährleisten und die Organisation aufrechtzuerhalten;
- Sicherstellung, dass alle relevanten Mitarbeiter eine jährliche AML-Schulung absolvieren.

Die erste Verteidigungslinie - die Mitarbeiter

Die erste Verteidigungslinie hat die Aufgabe, die Sorgfaltspflichten bei der Aufnahme einer Geschäftsbeziehung und die Sorgfaltspflichten während der Geschäftsbeziehung anzuwenden. Die erste Verteidigungslinie umfasst die Struktureinheiten und Mitarbeiter des Unternehmens, mit deren Aktivitäten Risiken verbunden sind und die diese Risiken, ihre spezifischen Merkmale und ihr Ausmaß identifizieren und bewerten müssen und die diese Risiken im Rahmen ihrer gewöhnlichen Aktivitäten verwalten, vor allem durch die Anwendung von Sorgfaltsmaßnahmen. Die Risiken, die sich aus den Aktivitäten und der Erbringung von Dienstleistungen des Unternehmens ergeben, gehören zur ersten Verteidigungslinie. Sie sind die Manager (Eigentümer) dieser Risiken und für sie verantwortlich.

[8] Zum Zweck der Vereinfachung dieser Leitlinien umfasst der Begriff "AML" auch die Verhinderung der Terrorismusfinanzierung und die Umsetzung von Sanktionen

Die Mitarbeiter des Unternehmens müssen mit der von ihnen erwarteten Voraussicht und Kompetenz und gemäß den für ihre Positionen festgelegten Anforderungen handeln, ausgehend von den Interessen und Zielen des Unternehmens, und sicherstellen, dass das Finanzsystem und der Wirtschaftsraum des Landes nicht für Geldwäsche und Terrorismusfinanzierung genutzt werden. Das Unternehmen ergreift Maßnahmen, um die Eignung der Mitarbeiter zu beurteilen, bevor sie ihre Arbeit aufnehmen, und bietet ihnen eine entsprechende Schulungan.

Aus den vorgenannten Gründen sind die Mitarbeiter verpflichtet,:

- alle in den Richtlinien und anderen zugehörigen Dokumenten aufgeführten Anforderungen einhalten;
- die erforderlichen Kundeninformationen in Übereinstimmung mit ihrer Funktion und ihren Verantwortlichkeiten sammeln;
- Informationen, Situationen, Aktivitäten, Transaktionen oder versuchte Transaktionen, die für jede Art von Dienstleistung oder Kundenbeziehung ungewöhnlich sind, unabhängig von der Höhe des Betrags und unabhängig davon, ob die Transaktion unverzüglich abgeschlossen wurde oder nicht, an die MLRO zu melden;
- Kunden nicht informieren oder anderweitig darauf aufmerksam machen, wenn der Kunde oder andere Kunden Gegenstand einer Meldung sind oder sein könnten oder wenn eine Meldung eingereicht wurde oder werden könnte;
- die entsprechende AML-Schulung absolvieren, die für die Position des Mitarbeiters erforderlich ist.

Die zweite Verteidigungslinie - Risikomanagement und Compliance, MLRO

Die zweite Verteidigungslinie besteht aus den Funktionen Risikomanagement und Compliance. Diese Funktionen können auch von ein und derselben Person oder Struktureinheit wahrgenommen werden, je nach Größe des Unternehmens und der Art, dem Umfang und dem Grad der Komplexität ihrer Aktivitäten und erbrachten Dienstleistungen, einschließlich der Risikobereitschaft und der Risiken, die sich aus den Aktivitäten des Unternehmens ergeben.

Ziel der **Compliance-Funktion** ist es, zu gewährleisten, dass das Unternehmen die geltenden Gesetze, Richtlinien und sonstigen Dokumente einhält, und die möglichen Auswirkungen von Änderungen des rechtlichen oder regulativen Umfelds auf die Aktivitäten des Unternehmens und auf den Compliance-Rahmen zu bewerten. Die Aufgabe von Compliance besteht darin, die erste Verteidigungslinie als Risikoeigentümer dabei zu unterstützen, die Orte zu definieren, an denen sich Risiken manifestieren (z.B. Analyse verdächtiger und ungewöhnlicher Transaktionen, wofür die Compliance-Mitarbeiter über die erforderlichen fachlichen Fähigkeiten, persönlichen Qualitäten usw. verfügen) und der ersten Verteidigungslinie zu helfen, diese Risiken effizient zu managen. Die zweite Verteidigungslinie geht keine Risiken ein.

Die Risikopolitik wird umgesetzt, und der Rahmen für das Risikomanagement wird von der **Risikomanagement-Funktion** kontrolliert. Der Ausführende der Risikomanagementfunktion stellt sicher, dass alle Risiken identifiziert, bewertet, gemessen, überwacht und gesteuert werden, und informiert die entsprechenden Einheiten des Unternehmens darüber. Der Ausführende der Risikomanagementfunktion für die Zwecke der Geldwäschebekämpfung beaufsichtigt in erster Linie die Einhaltung der Risikobereitschaft, die Risikotoleranz, die Identifizierung von Risikoveränderungen, gibt einen Überblick über die damit verbundenen Risiken und nimmt andere Aufgaben im Zusammenhang mit dem Risikomanagement wahr.

Der Vorstand hat einen **MLRO** für die Wahrnehmung der Funktionen der zweiten Verteidigungslinie ernannt. Diese Person ist nicht operativ in die Bereiche involviert, die der MLRO überwachen und überprüfen wird, und ist daher in Bezug auf diese unabhängig.

Innerhalb des derzeitigen AML-Rahmens des Unternehmens ist es der MLRO, der die wichtigsten Entscheidungen in Bezug auf einzelne AML-Fragen trifft, wie z.B. die Genehmigung von PEPs, die Annahme oder Ablehnung von Benutzern mit hohem Risiko usw. Der ernannte AML-Beauftragte des Unternehmens ist der leitende Angestellte des Unternehmens und eine Person, die über alle erforderlichen Kenntnisse und einen entsprechenden beruflichen Hintergrund verfügt.

Der MLRO ist für die folgenden Aktivitäten verantwortlich:

- die Richtlinien des Unternehmens zu erstellen und, wenn nötig, zu aktualisieren;
- laufend zu überwachen und zu überprüfen, ob das Unternehmen die in diesen Richtlinien und den dazugehörigen Dokumenten vorgeschriebenen Anforderungen sowie die externen Gesetze und Vorschriften erfüllt;
- die Mitarbeiter des Unternehmens und die Mitglieder des Vorstands in Bezug auf die Vorschriften zur Geldwäsche und Terrorismusfinanzierung zu beraten und zu unterstützen;
- die Mitglieder des Verwaltungsrats und die relevanten Personen über die Vorschriften zur Geldwäsche und Terrorismusfinanzierung zu informieren und zu schulen;
- untersuchen und registrieren Sie ausreichende Daten über eingegangene interne Meldungen und entscheiden Sie, ob die Aktivität gerechtfertigt ist oder ob sie verdächtig ist;
- die entsprechenden Berichte bei den zuständigen Aufsichtsbehörden in Übereinstimmung mit den geltenden Rechtsvorschriften einreichen;
- zu prüfen und regelmäßig zu bewerten, ob die Verfahren und Richtlinien des Unternehmens zur Verhinderung der Nutzung des Unternehmens für Geldwäsche oder Terrorismusfinanzierung zweckmäßig und wirksam sind.

Der MLRO erstattet dem Vorstand vierteljährlich Bericht. Dieser Bericht muss schriftlich erfolgen und mindestens die folgenden Punkte enthalten:

- Anzahl der Kunden unter allen Risikoklassifizierungen
- Anzahl der Treffer von Personen in Bezug auf die Sanktionslisten und angewandten Maßnahmen;
- Anzahl der Kunden oder Vertreter von Kunden, die als PEPs oder Personen mit einer Verbindung zu einem PEP identifiziert wurden;

- Anzahl der internen Benachrichtigungen über verdächtige Aktivitäten oder Transaktionen;
- Anzahl der relevanten Berichte, die an den Financial Crime Investigation Service (FCIS) gemeldet wurden;
- Alle von der Kontrollfunktion festgestellten Unzulänglichkeiten (falls vorhanden) behoben wurden;
- Liste der obligatorischen Schulungen, die für die Mitarbeiter in Bezug auf AML-Maßnahmen durchgeführt wurden.
- Nummer und Inhalt eines Auskunftsersuchens an das FCIS im Rahmen einer Untersuchung;
- Die Bestätigung, dass die Risikobewertung des Unternehmens für Geldwäsche und Terrorismusfinanzierung auf dem neuesten Stand ist;
- Die Bestätigung, dass diese Richtlinien und andere damit verbundene Dokumente auf dem neuesten Stand sind;
- Die Bestätigung, dass die Personalausstattung in Bezug auf die AML-Maßnahmen ausreichend ist;

Die dritte Verteidigungslinie - Interne Revision

Die dritte Verteidigungslinie besteht aus einer unabhängigen und effektiven internen Auditfunktion. Die Funktion der Innenrevision kann von einem internen Kontrollbeauftragten wahrgenommen werden. Es kann sich dabei um einen oder mehrere Mitarbeiter, die strukturelle Einheit des Unternehmens mit den entsprechenden Funktionen oder um eine dritte Partei handeln, die die entsprechende Dienstleistung für das Unternehmen erbringt. Ein interner Kontrollbeauftragter darf nicht die Position eines MLRO und/oder eines Vorstandsmitglieds des Unternehmens oder eine andere Position innehaben, zu deren Aufgaben die Ausarbeitung und/oder Bearbeitung der internen Vorschriften und Richtlinien des Unternehmens zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung gehört.

Die Mitarbeiter, die strukturelle Einheit des Unternehmens oder Dritte, die die Funktion der Innenrevision ausüben, müssen über die erforderlichen Kompetenzen, Instrumente und den Zugang zu den relevanten Informationen in allen strukturellen Einheiten des Unternehmens verfügen. Die Methoden der Innenrevision müssen der Größe des Unternehmens, der Art, dem Umfang und dem Grad der Komplexität der Aktivitäten und der erbrachten Dienstleistungen entsprechen, einschließlich der Risikobereitschaft und der Risiken, die sich aus den Aktivitäten des Unternehmens ergeben.

Die Entscheidung, eine interne Revision durchzuführen, wird durch einen Beschluss des Vorstands getroffen. Der Vorstand muss die Notwendigkeit der Durchführung einer internen Revision mindestens einmal jährlich beurteilen.

GRUNDSÄTZE DER UMSETZUNG VON MASSNAHMEN ZUR SORGFALTSPFLICHT GEGENÜBER KUNDEN

Maßnahmen zur Sorgfaltspflicht gegenüber Kunden (Customer Due Diligence, CDD) sind erforderlich, um die Identität eines neuen oder bestehenden Kunden im Rahmen einer gut funktionierenden risikobasierten laufenden Überwachung der Geschäftsbeziehung mit dem Kunden zu überprüfen. Die CDD-Maßnahmen bestehen aus 3 Stufen, einschließlich vereinfachter und erweiterter Sorgfaltspflichten, wie unten angegeben.

Wichtigste Grundsätze

Die CDD-Maßnahmen werden in dem Umfang ergriffen und durchgeführt, der unter Berücksichtigung des Risikoprofils des Kunden und anderer Umstände in den folgenden Fällen erforderlich ist:

- bei Aufnahme der Geschäftsbeziehung und während der laufenden Überwachung der Geschäftsbeziehung;
- bei der Ausführung oder Vermittlung gelegentlicher Transaktionen außerhalb der Geschäftsbeziehung, wenn der Wert der Transaktion(en) 700 Euro oder mehr (oder einen gleichwertigen Betrag in einem anderen Vermögenswert) innerhalb von 24 Stunden beträgt;
- bei der Durchführung oder Vermittlung von gelegentlichen Transaktionen außerhalb der Geschäftsbeziehung, wenn der Wert der Transaktion(en) innerhalb eines Monats 10.000 Euro oder mehr (oder einen gleichwertigen Betrag in anderen Vermögenswerten) beträgt;
- bei der Überprüfung von Informationen, die bei der Anwendung von Sorgfaltspflichten gesammelt wurden, oder im Falle von Zweifeln an der Hinlänglichkeit oder dem Wahrheitsgehalt der zuvor gesammelten Dokumente oder Daten bei der Aktualisierung der relevanten Daten;
- bei Verdacht auf Geldwäsche oder Terrorismusfinanzierung, unabhängig von den in diesen Richtlinien und der geltenden Gesetzgebung vorgesehenen Ausnahmen, Befreiungen oder Beschränkungen.

Das Unternehmen baut die Geschäftsbeziehung nicht auf oder unterhält sie nicht und führt die Transaktion nicht durch, wenn:

- das Unternehmen nicht in der Lage ist, eine der erforderlichen CDD-Maßnahmen zu ergreifen und durchzuführen;
- das Unternehmen den Verdacht hat, dass die Dienstleistungen oder Transaktionen des Unternehmens für Geldwäsche oder Terrorismusfinanzierung genutzt werden;
- das Risikoniveau des Kunden oder der Transaktion nicht mit der Risikobereitschaft des Unternehmens übereinstimmt.

Im Falle des Erhalts von Informationen in Fremdsprachen im Rahmen der CDD-Umsetzung kann das Unternehmen eine Übersetzung der Dokumente in eine andere für das Unternehmen geeignete Sprache verlangen. Die Verwendung von Übersetzungen sollte in Situationen vermieden werden, in denen die Originaldokumente in einer für das Unternehmen geeigneten Sprache verfasst sind.

Das Erreichen von CDD ist ein Prozess, der mit der Umsetzung von CDD-Maßnahmen beginnt. Wenn dieser Prozess abgeschlossen ist, wird dem Kunden eine dokumentierte individuelle Risikostufe zugewiesen, die die Grundlage für Folgemaßnahmen bildet und die bei Bedarf weiterverfolgt und aktualisiert wird.

Das Unternehmen hat CDD-Maßnahmen angemessen angewandt, wenn das Unternehmen die innere Überzeugung hat, dass es der Verpflichtung zur Anwendung von Sorgfaltsmaßnahmen nachgekommen ist. Bei der Prüfung der inneren Überzeugung wird der Grundsatz der Angemessenheit beachtet. Das bedeutet, dass das Unternehmen bei der Anwendung von CDD-Maßnahmen die Kenntnis, das Verständnis und die Behauptung erlangen muss, dass es genügend Informationen über den Kunden, die Aktivitäten des Kunden, den Zweck der Geschäftsbeziehung und der im Rahmen der Geschäftsbeziehung durchgeführten Transaktionen, die Herkunft der Gelder usw. gesammelt hat, so dass es den Kunden und die (geschäftlichen) Aktivitäten des Kunden versteht und dabei das Risikoniveau des Kunden, das mit der Geschäftsbeziehung verbundene Risiko und die Art dieser Beziehung berücksichtigt. Ein solches Maß an Behauptung muss es ermöglichen, komplizierte, hochwertige und ungewöhnliche Transaktionen und Transaktionsmuster zu erkennen, die keinen vernünftigen oder offensichtlichen wirtschaftlichen oder legitimen Zweck haben oder für die Besonderheiten des betreffenden Geschäfts untypisch sind.

Das Unternehmen muss die CDD nicht nur auf natürliche, sondern auch auf juristische Personen anwenden. Alle Gegenparteien und Partner des Unternehmens werden vom MLRO-Beauftragten mit Hilfe von zuverlässigen und unabhängigen Quellen manuell überprüft.

Die angebotenen Dienstleistungen

Die Haupttätigkeit des Unternehmens sind die Dienstleistungen für virtuelle Währungen. Aus diesem Grund bietet das Unternehmen seinen Kunden die folgenden Transaktionsarten an:

- die Bereitstellung eines Betreibers für den Umtausch virtueller Währungen, der es dem Kunden ermöglicht, virtuelle Währungen zu tauschen, zu kaufen und zu verkaufen.

Das Unternehmen erbringt die vorgenannten Leistungen nur im Rahmen einer bestehenden Geschäftsbeziehung.

Die Überprüfung der für die Identifizierung des Kunden verwendeten Informationen

Die Überprüfung der Informationen zur Identifizierung des Kunden bedeutet die Verwendung von Daten aus einer zuverlässigen und unabhängigen Quelle, um zu bestätigen, dass die Daten wahr und richtig sind, und gegebenenfalls auch zu bestätigen, dass die Daten, die sich direkt auf den Kunden beziehen, wahr und richtig sind.

Dies bedeutet unter anderem, dass der Zweck der Überprüfung von Informationen darin besteht, die Gewissheit zu erlangen, dass der Kunde, der die Geschäftsbeziehung aufnehmen möchte, die Person ist, die er vorgibt zu sein.

Das Unternehmen baut die Geschäftsbeziehung nicht auf oder unterhält sie nicht und führt die Transaktion nicht durch, wenn:

- die aus zwei verschiedenen Quellen stammen;
- die von einem Dritten oder einer Stelle ausgestellt (Ausweisdokumente) oder erhalten wurden, die kein Interesse an oder keine Verbindung zum Kunden oder zum Unternehmen hat, d.h. die neutral sind (z.B. sind Informationen aus dem Internet keine solchen Informationen, da sie oft vom Kunden selbst stammen oder ihre Zuverlässigkeit und Unabhängigkeit nicht überprüft werden kann);
- deren Zuverlässigkeit und Unabhängigkeit ohne objektive Hindernisse festgestellt werden kann und deren Zuverlässigkeit und Unabhängigkeit auch für einen nicht an der Geschäftsbeziehung beteiligten Dritten nachvollziehbar ist; und
- die darin enthaltenen oder über sie erhaltenen Daten aktuell und sachdienlich sind und das Unternehmen sich hierüber vergewissern kann (und in bestimmten Fällen auch auf der Grundlage der beiden vorstehenden Klauseln vergewissern kann).

Anwendung von vereinfachten Sorgfaltspflichten (Stufe 1)

Vereinfachte Sorgfaltspflichten (SDD) werden angewendet, wenn das Risikoprofil des Kunden auf ein geringes ML/TF-Risiko hinweist.

Bei der Anwendung von SDD-Maßnahmen darf das Unternehmen nur[9] die folgenden Daten des Kunden, der eine natürliche Person ist, erhalten:

- Name(n) und Nachname(n);
- persönliche Nummer;[10] oder

im Falle des Kunden, der eine juristische Person ist, die folgenden Daten:

- Geschäftsname oder Name;
- Rechtsform;
- Registrierungsnummer, falls eine solche Nummer vergeben wurde;
- Hauptsitz (Adresse) und Adresse des tatsächlichen Betriebs;
- Name(n), Nachname(n) und Personennummer oder Geburtsdatum des Vertreters des Kunden; und

sicherstellen, dass die erste Zahlung über ein Konto bei einem Kreditinstitut erfolgt, das im EWR oder in einem Drittland registriert ist, das Anforderungen stellt, die den in den einschlägigen Gesetzen festgelegten gleichwertig sind, und das von den zuständigen Behörden auf die Einhaltung dieser Anforderungen überwacht wird.

SDD-Maßnahmen dürfen nur durchgeführt werden, wenn die laufende Überwachung der Geschäftsbeziehung des Kunden in Übereinstimmung mit den Richtlinien erfolgt und die Möglichkeit besteht, verdächtige Geldgeschäfte und Transaktionen zu identifizieren.

SDD-Maßnahmen dürfen nicht unter den Umständen durchgeführt werden, unter denen verstärkte Sorgfaltspflichtmaßnahmen (wie unten beschrieben) durchgeführt werden müssen.

---

9 Wenn es sich bei dem Kunden um eine staatliche oder kommunale Einrichtung oder Behörde oder die Bank von Litauen handelt, kann das Unternehmen im Zuge der Anwendung von SDD-Maßnahmen nur die persönlichen Daten dieser Einrichtungen und ihrer Vertreter erfassen

10 im Falle eines Ausländers - Geburtsdatum (falls vorhanden - Personennummer oder eine andere eindeutige Zeichenfolge, die dieser Person zur persönlichen Identifizierung gewährt wird).

Wenn im Zuge der laufenden Überwachung der Geschäftsbeziehungen des Kunden festgestellt wird, dass das Risiko von Geldwäsche und/oder Terrorismusfinanzierung nicht mehr gering ist, muss das Unternehmen die entsprechenden CDD-Maßnahmen ergreifen.

Anwendung von Standard-Due-Diligence-Maßnahmen (Stufe 2)

Die Standard-Due-Diligence-Maßnahmen werden auf alle Kunden angewandt, bei denen CDD-Maßnahmen in Übereinstimmung mit den Richtlinien angewandt werden müssen. Die folgenden Standard-Due-Diligence-Maßnahmen sollten angewendet werden:

- die Identifizierung des Kunden und die Überprüfung der übermittelten Informationen auf der Grundlage von Informationen, die von einer zuverlässigen und unabhängigen Quelle stammen;
- Identifizierung und Überprüfung eines Vertreters des Kunden und dessen Vertretungsberechtigung;
- die Identifizierung des wirtschaftlichen Eigentümers und, zum Zweck der Überprüfung seiner Identität, die Ergreifung von Maßnahmen in einem Umfang, der es dem Unternehmen ermöglicht, sich zu vergewissern, dass es weiß, wer der wirtschaftliche Eigentümer ist, und die Eigentums- und Kontrollstruktur des Kunden versteht;
- Verständnis der Geschäftsbeziehung, der Transaktion oder des Vorgangs und, soweit relevant, Einholung von Informationen darüber;
- das Sammeln von Informationen darüber, ob es sich bei dem Kunden um einen PEP, ein Familienmitglied oder eine Person handelt, von der bekannt ist, dass sie ihm nahe steht;
- die Überwachung der Geschäftsbeziehung.

Die oben genannten CDD-Maßnahmen müssen vor der Aufnahme der Geschäftsbeziehung oder der Durchführung einer Transaktion angewendet werden. Die genauen Anweisungen für die Anwendung der Standard-Due-Diligence-Maßnahmen finden Sie in den Richtlinien.

Anwendung erweiterter Sorgfaltspflichtmaßnahmen (Stufe 3)

Zusätzlich zu den Standard-Due-Diligence-Maßnahmen wendet das Unternehmen verstärkte Due-Diligence-Maßnahmen (EDD) an, um ein festgestelltes Risiko der Geldwäsche und Terrorismusfinanzierung zu verwalten und zu mindern, wenn das Risiko höher als üblich ist.

Das Unternehmen wendet EDD-Maßnahmen immer dann an, wenn:

- das Risikoprofil des Kunden deutet auf ein hohes Risiko von ML / TF hin;
- nach der Identifizierung des Kunden oder der Überprüfung der übermittelten Informationen Zweifel an der Wahrhaftigkeit der übermittelten Daten, der Echtheit der Dokumente oder der Identifizierung des wirtschaftlichen Eigentümers bestehen;
- wenn grenzüberschreitende Korrespondenzbeziehungen mit dem Kunden, der ein Finanzinstitut aus einem Drittland ist, aufgenommen werden;
- im Falle der Durchführung einer Transaktion oder einer Geschäftsbeziehung mit dem PEP das Familienmitglied des PEP oder eine Person, von der bekannt ist, dass sie eine enge Beziehung zum PEP hat;
- wenn Transaktionen oder Geschäftsbeziehungen mit natürlichen Personen mit Wohnsitz oder juristischen Personen mit Sitz in Drittländern mit hohem Risiko, die von der Europäischen Kommission identifiziert wurden, durchgeführt werden;

- der Kunde aus einem solchen Land oder Gebiet stammt oder sein Wohnsitz oder Sitz oder der Sitz des Zahlungsdienstleisters des Zahlungsempfängers sich in einem Land oder Gebiet befindet, das nach glaubwürdigen Quellen wie gegenseitigen Bewertungen, Berichten oder veröffentlichten Folgeberichten keine wirksamen AML/CFT-Systeme eingerichtet hat, die den Empfehlungen der FATF entsprechen.

Vor der Anwendung von EDD-Maßnahmen stellt der Mitarbeiter des Unternehmens sicher, dass die Geschäftsbeziehung oder Transaktion ein hohes Risiko aufweist und dass dieser Geschäftsbeziehung oder Transaktion ein hohes Risiko zugeordnet werden kann. Vor allem prüft der Mitarbeiter vor der Anwendung der EDD-Maßnahmen, ob die oben beschriebenen Merkmale vorhanden sind und wendet sie als unabhängige Gründe an (d.h. jeder der identifizierten Faktoren erlaubt die Anwendung von EDD-Maßnahmen in Bezug auf den Kunden).

Bei der Anwendung von EDD-Maßnahmen, wenn eine grenzüberschreitende Korrespondenzbeziehung mit dem Kunden, bei dem es sich um ein Finanzinstitut aus einem Drittland handelt, aufgenommen wird, muss das Unternehmen die folgenden Maßnahmen ergreifen:

- ausreichende Informationen über den Kunden zu sammeln, um die Art seiner Geschäftstätigkeit vollständig zu verstehen und aus öffentlich zugänglichen Informationen den Ruf des Kunden und die Qualität der Überwachung zu ermitteln;
- Kontrollmechanismen für AML des Kunden und der Einrichtung, die Gelder erhält, zu bewerten;
- vor der Aufnahme neuer Korrespondenzbeziehungen die Genehmigung des Vorstandsmitglieds einholen;
- dokumentieren die jeweiligen Verantwortlichkeiten des Kunden;
- sich vergewissern, dass der Kunde eine ordnungsgemäße Sorgfaltsprüfung durchgeführt hat (einschließlich der Überprüfung der Identität der Kunden, die direkten Zugang zu den Konten des Kunden haben, und der Durchführung anderer Sorgfaltsprüfungsmaßnahmen) und dass er in der Lage ist, dem Unternehmen auf dessen Anfrage die relevanten Kundenidentifikationsdaten zur Verfügung zu stellen.

Bei der Anwendung von EDD-Maßnahmen muss das Unternehmen in Fällen, in denen Transaktionen oder Geschäftsbeziehungen mit dem PEP, einem Familienmitglied des PEP oder einer Person, von der bekannt ist, dass sie dem PEP nahe steht, durchgeführt werden, die folgenden Maßnahmen ergreifen:

- die Genehmigung des Vorstandsmitglieds einholen, bevor er eine Geschäftsbeziehung mit diesem Kunden aufnimmt oder die Geschäftsbeziehung mit dem Kunden fortsetzt, wenn dieser ein PEP wird;
- angemessene Maßnahmen ergreifen, um die Quelle des Vermögens und die Quelle der Gelder zu ermitteln, die an der Geschäftsbeziehung oder Transaktion beteiligt sind;
- eine fortlaufende Überwachung der Geschäftsbeziehung mit dem Kunden durchführen, indem Sie die Anzahl und den Zeitpunkt der durchgeführten Kontrollen erhöhen und Muster von Transaktionen auswählen, die einer weiteren Prüfung bedürfen.

Bei der Anwendung von EDD-Maßnahmen in Fällen, in denen Transaktionen oder Geschäftsbeziehungen mit natürlichen Personen mit Wohnsitz oder juristischen Personen mit Sitz in von der Europäischen Kommission identifizierten Hochrisiko-Drittländern durchgeführt werden, muss das Unternehmen die folgenden Maßnahmen anwenden:

- die Einholung zusätzlicher Informationen über den Kunden und seinen wirtschaftlichen Eigentümer;
- die Einholung zusätzlicher Informationen über die beabsichtigte Art der Geschäftsbeziehung;
- Einholung von Informationen über die Herkunft der Gelder und des Vermögens des Kunden und seines wirtschaftlichen Eigentümers;
- die Einholung von Informationen über die Gründe für die beabsichtigten oder durchgeführten Transaktionen;
- Einholung der Zustimmung des Vorstandsmitglieds für die Aufnahme von Geschäftsbeziehungen mit dem Kunden oder die Fortsetzung von Geschäftsbeziehungen mit ihm;
- eine fortlaufende Überwachung der Geschäftsbeziehung mit dem Kunden durchführen, indem Sie die Anzahl und den Zeitpunkt der durchgeführten Kontrollen erhöhen und Muster von Transaktionen auswählen, die einer weiteren Prüfung bedürfen;
- sicherzustellen, dass die erste Zahlung über ein auf den Namen des Kunden lautendes Konto bei einem Kreditinstitut abgewickelt wird, das im EWR oder in einem Drittland registriert ist, das Anforderungen stellt, die denen des geltenden Rechts gleichwertig sind, und das von den zuständigen Behörden auf die Einhaltung dieser Anforderungen überwacht wird.

Bei der Anwendung von EDD-Maßnahmen, wenn der Kunde aus einem solchen Land oder Gebiet stammt oder sein Wohnsitz oder Sitz oder der Sitz des Zahlungsdienstleisters des Zahlungsempfängers sich in einem Land oder Gebiet befindet, das nach glaubwürdigen Quellen wie gegenseitigen Bewertungen, Berichten oder veröffentlichten Folgeberichten keine wirksamen Systeme zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung eingerichtet hat, die mit den Empfehlungen der FATF übereinstimmen, muss die Gesellschaft die folgenden Maßnahmen anwenden:

- Einholung der Zustimmung des Vorstandsmitglieds für die Aufnahme von Geschäftsbeziehungen mit dem Kunden oder die Fortsetzung von Geschäftsbeziehungen mit ihm;
- Einholung von Informationen über die Herkunft der Gelder und des Vermögens des Kunden und seines wirtschaftlichen Eigentümers;
- eine fortlaufende Überwachung der Geschäftsbeziehung mit dem Kunden durchführen, indem Sie die Anzahl und den Zeitpunkt der durchgeführten Kontrollen erhöhen und Muster von Transaktionen auswählen, die einer weiteren Prüfung bedürfen;

In allen anderen Fällen, in denen EDD-Maßnahmen angewandt werden müssen, werden der Umfang und das Ausmaß der EDD-Maßnahmen von dem Mitarbeiter bestimmt, der diese Maßnahmen durchführt. Die folgenden zusätzlichen und relevanten Sorgfaltspflichtmaßnahmen können angewendet werden:

- Überprüfung der zusätzlich eingereichten Informationen nach Identifizierung des Kunden auf der Grundlage zusätzlicher Dokumente, Daten oder Informationen, die aus einer glaubwürdigen und unabhängigen Quelle stammen;
- Einholung zusätzlicher Informationen über den Zweck und die Art der Geschäftsbeziehung oder Transaktion und Überprüfung der übermittelten Informationen anhand zusätzlicher Dokumente, Daten oder Informationen, die aus einer zuverlässigen und unabhängigen Quelle stammen;
- die Einholung zusätzlicher Informationen und Dokumente über die tatsächliche Ausführung der im Rahmen der Geschäftsbeziehung getätigten Transaktionen, um die Scheinbarkeit der Transaktionen auszuschließen;
- die Einholung zusätzlicher Informationen und Dokumente, um die Quelle und Herkunft der Gelder zu ermitteln, die für eine Transaktion im Rahmen der Geschäftsbeziehung verwendet wurden, um die Anscheinsbeweise für die Transaktionen auszuschließen;
- die Durchführung der ersten Zahlung im Zusammenhang mit einer Transaktion über ein Konto, das

auf den Namen des an der Transaktion beteiligten Kunden bei einem Kreditinstitut eröffnet werden, das in einem Vertragsstaat des Europäischen Wirtschaftsraums oder in einem Land, in dem Anforderungen gelten, die denen der Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates entsprechen, registriert ist oder dort seinen Sitz hat;

- die Anwendung von CDD-Maßnahmen in Bezug auf den Kunden oder seinen Vertreter, während er sich am selben Ort wie der Kunde oder sein Vertreter befindet;
- Einholung zusätzlicher Informationen über den Kunden und seinen wirtschaftlichen Eigentümer, einschließlich der Identifizierung aller Eigentümer des Kunden, einschließlich derjenigen, deren Anteil unter 25% liegt;
- das Sammeln von Informationen über die Herkunft der Gelder und des Vermögens des Kunden und seines wirtschaftlichen Eigentümers;
- Verbesserung der Überwachung der Geschäftsbeziehung durch Erhöhung der Anzahl und Häufigkeit der angewandten Kontrollmaßnahmen und durch Auswahl von Transaktionsindikatoren oder Transaktionsmustern, die zusätzlich überprüft werden;
- Einholung der Genehmigung des Vorstandsmitglieds für die Durchführung von Transaktionen oder die Aufnahme von Geschäftsbeziehungen mit neuen und bestehenden Kunden;

Bei der Durchführung von EDD ist das Unternehmen in bestimmten Fällen verpflichtet, angemessene Maßnahmen zu ergreifen, um die Herkunft der Gelder und des Vermögens der Kunden zu ermitteln. Die Herkunft der Gelder kann *u.a. anhand* folgender Kriterien überprüft werden

- eine jährliche Steuererklärung;
- ein Original oder eine beglaubigte Kopie einer aktuellen Gehaltsabrechnung;
- eine vom Arbeitgeber unterzeichnete schriftliche Bestätigung des Jahresgehalts;
- ein Original oder eine beglaubigte Kopie des Kaufvertrags für die Immobilie und ein Originalauszug eines Finanzinstituts, der den Erhalt der aus dem Verkauf der Immobilie erhaltenen Mittel belegt, falls vorhanden;
- ein Original oder eine beglaubigte Kopie eines Testaments oder eines gleichwertigen Dokuments, das die Erbschaft belegt;
- ein Original oder eine beglaubigte Kopie einer Schenkungsvereinbarung (entweder in einfacher schriftlicher Form oder notariell beglaubigt, falls eine notarielle Form der Vereinbarung gesetzlich vorgeschrieben ist);
- ein Original oder eine beglaubigte Kopie eines Darlehensvertrags (entweder in einfacher schriftlicher Form oder notariell beglaubigt, wenn die notarielle Form des Vertrags gesetzlich vorgeschrieben ist) und ein Auszug aus einem Finanzinstitut, der den Empfang oder die Überweisung von Geldern im Zusammenhang mit der Aufnahme des Darlehens oder der Rückzahlung eines gewährten Darlehens belegt; oder ein Schuldschein (entweder in einfacher schriftlicher Form oder notariell beglaubigt, wenn die notarielle Form des Vertrags gesetzlich vorgeschrieben ist);

- eine Internetrecherche in einem Unternehmensregister, um den Verkauf eines Unternehmens zu bestätigen;
- das Original oder eine beglaubigte Kopie der Kautionsvereinbarung;
- Kassenbuch oder Register der Kassengeschäfte (für juristische Personen);
- weitere Informationen.

Der Mitarbeiter muss die angewandten EDD-Maßnahmen innerhalb von 2 Arbeitstagen nach Beginn der Anwendung der EDD-Maßnahmen melden, indem er eine entsprechende Mitteilung an den MLRO sendet.

Im Falle der Anwendung von EDD-Maßnahmen bewertet das Unternehmen das Risikoprofil des Kunden spätestens alle sechs Monate neu.

MASSNAHMEN ZUR SORGFALTSPFLICHT GEGENÜBER KUNDEN

Identifizierung des Kunden - natürliche Person

Das Unternehmen identifiziert den Kunden, bei dem es sich um eine natürliche Person handelt, und ggf. seinen Vertreter und speichert die folgenden Daten über den Kunden:

- Name(n) und Nachname(n);
- persönliche Nummer;[11]
- Bürgerschaft;[12]
- Foto;
- Unterschrift.[13]

Die folgenden gültigen Ausweisdokumente, die die oben genannten Daten enthalten, können als Grundlage für die Identifizierung einer natürlichen Person verwendet werden:

- ein Ausweisdokument der Republik Litauen mit Ausnahme der Aufenthaltsgenehmigung der Republik Litauen;
- ein Ausweisdokument eines ausländischen Staates;

Der Kunde, der eine natürliche Person ist, kann im Rahmen der Geschäftsbeziehung mit dem Unternehmen keinen Vertreter einsetzen.

Identifizierung des Kunden - juristische Person

Das Unternehmen identifiziert den Kunden, bei dem es sich um eine juristische Person und ihren Vertreter handelt, und speichert die folgenden Daten über den Kunden:

- Geschäftsname oder Name;
- Rechtsform;
- Registrierungsnummer, falls eine solche Nummer vergeben wurde;

---

[11] im Falle eines Ausländers - Geburtsdatum (falls vorhanden - Personennummer oder eine andere eindeutige Zeichenfolge, die dieser Person zur persönlichen Identifizierung gewährt wird);

[12] wenn ein Ausweisdokument keine Angaben zur Staatsangehörigkeit des Kunden enthält, müssen Finanzinstitute und andere Verpflichtete bei der Identifizierung des Kunden, der eine natürliche Person ist, in dessen physischer Anwesenheit vom Kunden die Angaben zur Staatsangehörigkeit verlangen.

[13] außer in den Fällen, in denen dies im Identitätsdokument fakultativ ist;

- Vorname(n) und Nachname(n), Personennummer (im Falle eines Ausländers - Geburtsdatum oder, falls vorhanden, Personennummer oder eine andere eindeutige Zeichenfolge, die dem

diese Person, die zur persönlichen Identifizierung bestimmt ist) und die Staatsangehörigkeit des/der Geschäftsführer(s) oder des/der Mitglieder des Vorstands oder des/der Mitglieder eines anderen gleichwertigen Organs sowie ihre Befugnisse bei der Vertretung des Kunden;

- einen Auszug aus der Registrierung und das Datum der Ausstellung;
- Hauptsitz (Adresse) und Adresse des tatsächlichen Betriebs
- Die folgenden Dokumente, die von einer zuständigen Behörde oder Stelle frühestens sechs Monate vor ihrer Verwendung ausgestellt wurden, können zur Identifizierung des Kunden herangezogen werden:
    - Registrierkarte des betreffenden Registers; oder
    - Eintragungsbescheinigung des zuständigen Registers; oder
    - ein Dokument, das einem der vorgenannten Dokumente gleichwertig ist, oder relevante Niederlassungsdokumente des Kunden.

Das Unternehmen prüft die Richtigkeit der oben genannten Daten des Kunden und verwendet zu diesem Zweck Informationen aus einer glaubwürdigen und unabhängigen Quelle. Wenn das Unternehmen Zugang zu dem entsprechenden Register für juristische Personen hat, muss die Vorlage der oben genannten Dokumente nicht vom Kunden verlangt werden.

Die Identität der juristischen Person und die Vertretungsbefugnis der juristischen Person können auf der Grundlage eines oben genannten Dokuments, das notariell beglaubigt oder amtlich beglaubigt wurde, oder auf der Grundlage anderer Informationen, die aus einer glaubwürdigen und unabhängigen Quelle stammen, einschließlich elektronischer Identifizierungsmittel und Vertrauensdienste für elektronische Transaktionen, überprüft werden, wobei in einem solchen Fall mindestens zwei verschiedene Quellen zur Überprüfung der Daten verwendet werden.

Die Identifizierung des Vertreters des Kunden und sein Recht auf Vertretung

Der Vertreter des Kunden muss als Kunde identifiziert werden, der eine natürliche Person im Sinne dieser Richtlinien ist. Das Unternehmen muss auch die Art und den Umfang des Vertretungsrechts des Kunden identifizieren und überprüfen. Der Name, das Ausstellungsdatum und der Name des Ausstellers des Dokuments, das als Grundlage für das Vertretungsrecht dient, müssen ermittelt und aufbewahrt werden, es sei denn, das Vertretungsrecht wurde anhand von Informationen aus dem entsprechenden Register überprüft.

Das Unternehmen muss die Bedingungen des Vertretungsrechts, das den Vertretern der juristischen Person gewährt wird, beachten und darf nur im Rahmen des Vertretungsrechts Dienstleistungen erbringen.

Die Vollmacht muss den Anforderungen des litauischen Zivilgesetzbuches entsprechen. Die im Ausland ausgestellte Vollmacht muss legalisiert oder mit einer Apostille versehen sein. Wenn die Vertretungsberechtigung des Kunden (der juristischen Person) aus dem Registerauszug, der Satzung oder gleichwertigen Dokumenten, die die Identität des Kunden (der juristischen Person) belegen, ersichtlich ist, sollte kein separates Dokument zur Bevollmächtigung (z.B. eine Vollmacht) erforderlich sein.

Die Identifizierung des wirtschaftlichen Eigentümers des Kunden

Das Unternehmen muss den wirtschaftlichen Eigentümer des Kunden identifizieren - eine Person, die den Kunden letztlich besitzt oder kontrolliert oder in deren Namen eine Transaktion durchgeführt wird. Das Unternehmen muss außerdem Maßnahmen ergreifen, um die Identität des wirtschaftlichen Eigentümers in einem Maße zu überprüfen, das es dem Unternehmen ermöglicht sicherzustellen, dass es weiß, wer der wirtschaftliche Eigentümer ist.

Das Unternehmen kann nicht davon ausgehen, dass die Privatpersonen selbst die BOs des Kunden sind, und muss immer zuerst die Informationen vom Kunden darüber einholen, wer der BO ist.

Die Identifizierung des BO bedeutet die Identifizierung einer natürlichen Person oder einer Gruppe von natürlichen Personen.

Das Unternehmen erhebt die folgenden Daten über den/die wirtschaftlich Berechtigten des Kunden:

- Name(n) und Nachname(n);
- persönliche Nummer;[14]
- Bürgerschaft.[15]

Das Unternehmen fordert vom Kunden Informationen zum wirtschaftlichen Eigentümer des Kunden an (z. B. indem es dem Kunden die Möglichkeit gibt, seinen wirtschaftlichen Eigentümer bei der Erfassung von Daten über den Kunden anzugeben).

Das Unternehmen nimmt die Geschäftsbeziehung nicht auf, wenn der Kunde, der eine natürliche Person ist, einen wirtschaftlichen Eigentümer hat, der nicht mit dem Kunden identisch ist.

Der wirtschaftliche Eigentümer einer juristischen Person wird in Stufen ermittelt, wobei der Verpflichtete zu jeder nachfolgenden Stufe übergeht, wenn der wirtschaftliche Eigentümer der juristischen Person in der vorherigen Stufe nicht ermittelt werden kann. Die Stufen sind wie folgt:

- ist es möglich, in Bezug auf den Kunden, bei dem es sich um eine juristische Person oder eine an der Transaktion beteiligte Person handelt, die natürliche(n) Person(en) zu identifizieren, die die juristische Person letztlich tatsächlich kontrolliert/kontrollieren oder in sonstiger Weise Einfluss oder Kontrolle über sie ausübt/ausüben, unabhängig von der Höhe der Anteile, Stimmrechte oder Eigentumsrechte oder ihrer direkten oder indirekten Natur;
- ob der Kunde, bei dem es sich um eine juristische Person handelt, oder die an der Transaktion beteiligte Person eine oder mehrere natürliche Personen hat, die die juristische Person über eine direkte[16] oder indirekte[17] Beteiligung besitzen oder kontrollieren. Auch familiäre und vertragliche Verbindungen müssen hier berücksichtigt werden;
- wer die natürliche Person in der obersten Führungsebene[18] ist, die als wirtschaftlicher Eigentümer definiert werden muss, da es dem Verpflichteten aufgrund der Ausführung der beiden vorangegangenen Schritte nicht möglich war, den wirtschaftlichen Eigentümer zu identifizieren.

Der Senior Manager des Kunden sollte nur in Ausnahmefällen als wirtschaftlicher Eigentümer angegeben werden, wenn das Unternehmen alle zumutbaren Anstrengungen unternimmt, um den wirtschaftlichen Eigentümer zu ermitteln, und wenn kein Grund für den Verdacht besteht, dass die Identität des wirtschaftlichen Eigentümers verschleiert wird. In diesem Fall sollte der Senior Manager als der Leiter (z.B. CEO) verstanden werden,

---

[14] im Falle eines Ausländers - Geburtsdatum (falls vorhanden - Personennummer oder eine andere eindeutige Zeichenfolge, die dieser Person zur persönlichen Identifizierung gewährt wird);

[15] wenn ein Ausweisdokument keine Angaben zur Staatsangehörigkeit des Kunden enthält, müssen Finanzinstitute und andere Verpflichtete bei der Identifizierung des Kunden, der eine natürliche Person ist, in dessen physischer Anwesenheit vom Kunden die Angaben zur Staatsangehörigkeit verlangen.

[16] **Direktes Eigentum** ist eine Art der Ausübung von Kontrolle, bei der die natürliche Person eine Beteiligung von 25 Prozent plus eine Aktie oder ein Eigentumsrecht von über 25 Prozent an dem Unternehmen besitzt.

[17] **Indirektes Eigentum** ist eine Art der Ausübung von Kontrolle, bei der eine 25-prozentige Beteiligung plus eine Aktie oder ein Eigentumsrecht von mehr als 25 Prozent an dem Unternehmen im Besitz eines Unternehmens ist,

das von einer natürlichen Person oder mehreren Unternehmen kontrolliert wird, die von derselben natürlichen Person kontrolliert werden.

[18] ein **Mitglied der Geschäftsleitung** ist eine Person, die die strategischen Entscheidungen trifft, die sich grundlegend auf die Geschäftsaktivitäten und/oder -praktiken und/oder die allgemeine (Geschäfts-)Entwicklung des Unternehmens auswirken, oder die in ihrer Abwesenheit alltägliche oder reguläre Managementfunktionen des Unternehmens im Rahmen der Exekutivgewalt ausübt (z. B. Chief Executive Officer (CEO), Chief Financial Officer (CFO), Direktor oder Präsident usw.).

Geschäftsführer, Leiter der Verwaltung) des Kunden.

Die für die Identifizierung der juristischen Person verwendeten Dokumente oder die anderen eingereichten Dokumente tun nicht direkt angeben, wer der wirtschaftliche Eigentümer der juristischen Person ist, werden die relevanten Daten (einschließlich der Daten über die Zugehörigkeit zu einer Gruppe und die Eigentums- und Verwaltungsstruktur der Gruppe) auf der Grundlage der Erklärung des Vertreters der juristischen Person oder des handschriftlichen Dokuments des Vertreters der juristischen Person registriert.

Das Unternehmen ergreift angemessene Maßnahmen, um die Richtigkeit der auf der Grundlage von Erklärungen oder eines handschriftlichen Dokuments ermittelten Informationen zu überprüfen (z. B. durch Nachfragen in den entsprechenden Registern), indem es die Vorlage des Jahresberichts der juristischen Person oder eines anderen relevanten Dokuments verlangt.

Bei der Identifizierung des wirtschaftlichen Eigentümers aufgetretene Schwierigkeiten

Die Gesellschaft sollte sich darüber im Klaren sein, dass die Angaben zum wirtschaftlichen Eigentum durch die Verwendung von Briefkastenfirmen, komplexen Eigentums- und Kontrollstrukturen mit vielen Schichten von Aktien, die auf den Namen anderer juristischer Personen eingetragen sind, nominierten Aktionären und Direktoren, wie z.B. engen Mitarbeitern und Familienangehörigen, und auf andere Weise verschleiert werden können.

In vielen Fällen besteht die Rolle der nominierten Direktoren und Anteilseigner darin, die Identität des BO und des Kontrolleurs eines Unternehmens oder Vermögenswerts zu schützen oder zu verbergen. Ein Nominee kann dazu beitragen, die gerichtlichen Kontrollen der Unternehmensbeteiligung zu überwinden und von Gerichten und Regierungsbehörden verhängte Verbote der Direktorenschaft zu umgehen. Das Unternehmen sollte sich daher besonders der Unternehmensstrukturen bewusst sein, die die Komplexität fördern und die Schwierigkeit erhöhen, genaue Informationen über den wirtschaftlichen Eigentümer zu erhalten. Darüber hinaus sollte sich das Unternehmen der Möglichkeit bewusst sein, dass es Nominee-Vereinbarungen gibt, bei denen Freunde, Familienmitglieder oder assoziierte Personen behaupten, die BOs von juristischen Personen, Rechtsvereinbarungen oder anderen Unternehmen zu sein.

Daher muss das Unternehmen geeignete und angemessene Maßnahmen ergreifen, um die wahren BOs zu ermitteln und Situationen zu identifizieren, in denen das wirtschaftliche Eigentum verschleiert wird.

Bei der Bestimmung des BO muss das Unternehmen Daten über die Eigentumsstruktur des Kunden sammeln und diese anhand von Dokumenten, Daten oder Informationen, die es aus einer zuverlässigen und unabhängigen Quelle erhalten hat, verifizieren. Im Falle einer Multi-Level-Ownership muss das Schema der Eigentümerstruktur vom Kunden erstellt oder vom Kunden eingeholt werden.

Das Unternehmen muss auch sicherstellen, dass es die Eigentums- und Kontrollstruktur des Kunden versteht, insbesondere wenn die Eigentums- und Kontrollstruktur komplex ist (z.B. wenn die Aktionäre aus mehreren verschiedenen Rechtsordnungen stammen, wenn die Aktionäre verschiedene Arten von juristischen Personen/Rechtsvereinbarungen haben, wenn es innerhalb der Eigentums- und Kontrollstruktur Trusts und private Investmentvehikel gibt, wenn der Kunde Inhaberaktien ausgegeben hat). Das Unternehmen muss beurteilen, ob die Eigentums- und Kontrollstruktur aus kommerzieller, wirtschaftlicher oder rechtlicher Sicht sinnvoll ist.

Nutzung des Informationssystems für juristische Personen Teilnehmer

Bei der Identifizierung eines wirtschaftlichen Eigentümers muss das Unternehmen zusätzlich das Informationssystem für Teilnehmer an juristischen Personen (JADIS) nutzen, aus dem es Daten über wirtschaftliche Eigentümer der Kunden und hat das Recht, andere staatliche Informationssysteme und Register zu nutzen, in denen Daten über die Teilnehmer von juristischen Personen gesammelt werden.
Der Zugang zu JADIS erfolgt über das Litauische Staatliche Unternehmensregisterzentrum (SECR) mittels der entsprechenden Anwendung. Der Antrag kann eingereicht werden:

- elektronisch über das Benutzer-Selbstbedienungssystem des Centre ofRegisters;
- per E-Mail info@registrucentras.lt, die mit einer elektronischen Signatur unterzeichnet werden sollte;
- in den Client Service Offices des Centre of Registers unter Vorlage des Originals.

Kunden und hat das Recht, andere staatliche Informationssysteme und Register zu nutzen, in denen Daten über die Teilnehmer von juristischen Personen gesammelt werden.

Der Zugang zu JADIS erfolgt über das Litauische Staatliche Unternehmensregisterzentrum (SECR) mittels der entsprechenden Anwendung. Der Antrag kann eingereicht werden:

- elektronisch über das Benutzer-Selbstbedienungssystem des Centre ofRegisters;
- per E-Mail info@registrucentras.lt, die mit einer elektronischen Signatur unterzeichnet werden sollte;
- in den Client Service Offices des Centre of Registers unter Vorlage des Originals.

Die vorbereiteten JADIS-Auszüge und Kopien von Dokumenten können sein:

- von der Selbstbedienung des Registerzentrums heruntergeladen werden (nur wenn der Antrag über die Selbstbedienung des Registerzentrums eingereicht wurde);
- bei den Kundenbetreuungsbüros des Centre ofRegisters abgeholt werden;
- per Post an die vom Kunden angegebene Adresse erhalten.

Nach der Feststellung einer Diskrepanz zwischen den in JADIS verfügbaren Informationen über die wirtschaftlichen Eigentümer des Kunden, der eine juristische Person ist, und den ihnen zur Verfügung stehenden Informationen über die wirtschaftlichen Eigentümer desselben Kunden, benachrichtigen Sie den Kunden darüber und schlagen ihm vor, dem Datenverarbeiter von JADIS korrekte Informationen über seine wirtschaftlichen Eigentümer zur Verfügung zu stellen.

Das Unternehmen darf keine Geschäftsbeziehung eingehen oder eine Transaktion durchführen (mit Ausnahme von Geldgeschäften oder Transaktionen, die im Rahmen einer Geschäftsbeziehung abgeschlossen und/oder durchgeführt werden), wenn die Angaben zu den wirtschaftlichen Eigentümern des Kunden, bei dem es sich um eine juristische Person handelt, nicht in JADIS enthalten sind oder wenn die in JADIS enthaltenen Angaben zu den wirtschaftlichen Eigentümern des Kunden, bei dem es sich um eine juristische Person handelt, falsch sind.

Identifikation der politisch exponierten Person

Die Gesellschaft ergreift Maßnahmen, um festzustellen, ob der Kunde, der wirtschaftliche Eigentümer des Kunden oder der Vertreter dieses Kunden ein PEP, ein Familienmitglied[19] oder ein enger Mitarbeiter[20] ist oder ob der Kunde eine solche Person geworden ist.

Das Unternehmen fordert vom Kunden Informationen an, um festzustellen, ob es sich bei dem Kunden um einen PEP, ein Familienmitglied oder einen engen Vertrauten handelt (z. B. indem es dem Kunden die Möglichkeit gibt, bei der Erfassung von Daten über den Kunden die relevanten Informationen anzugeben).

Das Unternehmen überprüft die vom Kunden erhaltenen Daten durch Abfragen in einschlägigen Datenbanken oder öffentlichen Datenbanken oder durch Abfragen oder Überprüfen von Daten auf den Websites der zuständigen Aufsichtsbehörden oder Institutionen des Landes, in dem der Kunde seinen Wohnsitz oder Sitz hat. PEP muss zusätzlich mit Hilfe einer internationalen Suchmaschine (z. B. Google) und gegebenenfalls der lokalen Suchmaschine des Herkunftslandes des Kunden überprüft werden, indem der Name des Kunden in lateinischer und lokaler Schrift mit dem Geburtsdatum des Kunden eingegeben wird.

Darüber hinaus wird das PEP-Status-Screening von der automatisierten AML-Lösung Sum & Substance implementiert und durchgeführt. Die Lösung bietet eine laufende Überprüfung des PEP-Status und identifiziert Familienmitglieder und enge Mitarbeiter der PEPs.

Mindestens die folgenden Personen gelten als PEPs:

- das Staatsoberhaupt, der Regierungschef, ein Minister, ein Vizeminister oder ein stellvertretender Minister, ein Staatssekretär, ein Kanzler des Parlaments, der Regierung oder eines Ministeriums;
- ein Mitglied des Parlaments;
- ein Mitglied des Obersten Gerichtshofs, des Verfassungsgerichts oder einer anderen obersten Justizbehörde, gegen deren Entscheidungen kein Rechtsmittel eingelegt werden kann;
- ein Bürgermeister der Gemeinde, ein Leiter der Gemeindeverwaltung;
- ein Mitglied des Leitungsgremiums der obersten staatlichen Rechnungs- oder Kontrollbehörde oder ein Vorsitzender, stellvertretender Vorsitzender oder ein Mitglied des Vorstands der Zentralbank;
- Botschafter ausländischer Staaten, ein Geschäftsträger ad interim, der Chef der litauischen Streitkräfte, der Kommandeur der Streitkräfte und Einheiten, der Chef des Verteidigungsstabs oder ein hoher Offizier ausländischer Streitkräfte;
- ein Mitglied des Verwaltungs- oder Aufsichtsorgans eines öffentlichen Unternehmens, einer Aktiengesellschaft oder einer Gesellschaft mit beschränkter Haftung, dessen Aktien oder ein Teil der Aktien, die mehr als 1/2 der gesamten Stimmen in der Hauptversammlung der Aktionäre dieser Unternehmen auf sich vereinigen, dem Staat gehören;

[19] **Familienangehörige**: der Ehepartner, die Person, mit der eine Partnerschaft eingetragen wurde (d.h. der Lebensgefährte), Eltern, Brüder, Schwestern, Kinder und die Ehepartner der Kinder, Lebensgefährten der Kinder

[20] **Eine nahe stehende Person** ist eine natürliche Person, die zusammen mit dem PEP Mitglied derselben juristischen Person oder einer Einrichtung ohne Rechtspersönlichkeit ist oder eine andere Geschäftsbeziehung unterhält; oder eine natürliche Person, die der einzige wirtschaftliche Eigentümer der juristischen Person oder einer Einrichtung ohne Rechtspersönlichkeit ist, die mit dem Ziel gegründet wurde oder de facto tätig ist, Eigentum oder einen anderen persönlichen Vorteil für den PEP zu erwerben.

- ein Mitglied des Verwaltungs- oder Aufsichtsorgans eines kommunalen Unternehmens, einer Aktiengesellschaft oder einer Gesellschaft mit beschränkter Haftung, deren Aktien oder ein Teil der Aktien, die mehr als 1/2 der Gesamtstimmen in der Hauptversammlung der Aktionäre dieser Unternehmen auf sich vereinen, sich im Besitz des Staates befinden und die als Großunternehmen im Sinne des Gesetzes über die Jahresabschlüsse von Unternehmen der Republik Litauen betrachtet werden;
- ein Direktor, ein stellvertretender Direktor oder ein Mitglied des Leitungs- oder Aufsichtsorgans einer internationalen zwischenstaatlichen Organisation;
- ein Vorsitzender, ein stellvertretender Vorsitzender oder ein Mitglied des Führungsgremiums einer politischen Partei.

Das Unternehmen identifiziert enge Mitarbeiter und Familienmitglieder von PEPs nur dann, wenn deren Verbindung zu PEPs der Öffentlichkeit bekannt ist oder wenn das Unternehmen Grund zu der Annahme hat, dass eine solche Verbindung besteht.

Wenn ein PEP nicht mehr mit einer prominenten öffentlichen Funktion betraut ist, muss die Gesellschaft innerhalb von 12 Monaten ab dem Datum des Ausscheidens des PEP aus den öffentlichen Funktionen die Risiken berücksichtigen, die mit dem Kunden verbunden bleiben. Nach einem Zeitraum von 12 Monaten ab dem Datum des Ausscheidens der PEP aus den öffentlichen Funktionen ist das Unternehmen verpflichtet, die mit diesem Kunden verbundenen Risiken neu zu bewerten.

Identifizierung des Zwecks und der Art der Geschäftsbeziehung oder einer Transaktion

Das Unternehmen muss den Zweck und die Art der Aufnahme der Geschäftsbeziehung oder der Durchführung der Transaktion verstehen. In Bezug auf die erbrachten Dienstleistungen kann das Unternehmen vom Kunden die folgenden Informationen anfordern, um den Zweck und die Art der Geschäftsbeziehung oder der Transaktion zu verstehen:

- ob der Kunde die Dienstleistungen des Unternehmens für seine eigenen Bedürfnisse nutzt oder die Interessen einer anderen Person vertritt;
- Kontaktinformationen;
- Informationen über die registrierte Adresse und die tatsächliche Wohnanschrift des Kunden;
- den geschätzten Transaktionsumsatz mit dem Unternehmen pro Kalenderjahr;
- die geschätzte Quelle der in der Geschäftsbeziehung oder Transaktion verwendeten Mittel;
- ob die Geschäftsbeziehung oder Transaktion mit der Ausübung wirtschaftlicher oder beruflicher Tätigkeiten des Kunden zusammenhängt und um welche Tätigkeiten es sich handelt;
- Informationen über die Herkunft der Mittel im Zusammenhang mit der Geschäftsbeziehung oder der Transaktion, wenn der Betrag der Transaktionen (einschließlich des erwarteten Betrags) das festgelegte Limit überschreitet.

[19] **Familienangehörige**: der Ehepartner, die Person, mit der eine Partnerschaft eingetragen wurde (d.h. der Lebensgefährte), Eltern, Brüder, Schwestern, Kinder und die Ehepartner der Kinder, Lebensgefährten der Kinder

[20] **Eine nahe stehende Person** ist eine natürliche Person, die zusammen mit dem PEP Mitglied derselben juristischen Person oder einer Einrichtung ohne Rechtspersönlichkeit ist oder eine andere Geschäftsbeziehung unterhält; oder eine natürliche Person, die der einzige wirtschaftliche Eigentümer der juristischen Person oder einer Einrichtung ohne Rechtspersönlichkeit ist, die mit dem Ziel gegründet wurde oder de facto tätig ist, Eigentum oder einen anderen persönlichen Vorteil für den PEP zu erwerben.

Das Unternehmen ergreift zusätzliche Maßnahmen und sammelt zusätzliche Informationen, um den Zweck und die Art der Geschäftsbeziehung zu identifizieren, wenn:

- es eine Situation gibt, die sich auf einen hohen Wert bezieht oder ungewöhnlich ist und/oder
- wenn das mit dem Kunden verbundene Risiko bzw. Risikoprofil und die Art der Geschäftsbeziehung die Durchführung zusätzlicher Maßnahmen erforderlich machen, um den Geschäftspartner angemessen überwachen zu können.

Überwachung der Geschäftsbeziehung

Das Unternehmen überwacht etablierte Geschäftsbeziehungen, bei denen die folgenden Maßnahmen zur laufenden Sorgfaltspflicht (periodisch) umgesetzt werden:

- Sicherstellung, dass die im Rahmen der Anwendung der Sorgfaltspflichtmaßnahmen gesammelten Dokumente, Daten oder Informationen regelmäßig und im Falle von auslösenden Ereignissen aktualisiert werden, d.h. vor allem die Daten über den Kunden, seinen Vertreter (einschließlich des Vertretungsrechts) und den wirtschaftlichen Eigentümer sowie den Zweck und die Art der Geschäftsbeziehung;
- die laufende Überwachung der Geschäftsbeziehung, die die im Rahmen der Geschäftsbeziehung durchgeführten Transaktionen umfasst, um sicherzustellen, dass die Transaktionen dem Wissen des Unternehmens über den Kunden, seine Aktivitäten und sein Risikoprofil entsprechen;
- Identifizierung der Quelle und Herkunft der für die Transaktion(en) verwendeten Mittel.

Das Unternehmen **prüft und aktualisiert** regelmäßig **die Dokumente, Daten und Informationen**, die im Rahmen der Durchführung von CDD-Maßnahmen gesammelt wurden, und aktualisiert das Risikoprofil des Kunden. Die Regelmäßigkeit der Kontrollen und der Aktualisierung muss sich nach dem Risikoprofil des Kunden richten und die Kontrollen müssen mindestens stattfinden:

- einmal halbjährlich für Kunden mit hohem Risikoprofil;
- einmal jährlich für den Kunden mit mittlerem Risikoprofil;
- einmal alle zwei Jahre für den Kunden mit niedrigem Risikoprofil.

Das Unternehmen hat ein System zur Speicherung, Systematisierung und Kontrolle der Kundenunterlagen eingeführt. Das System benachrichtigt den zuständigen Mitarbeiter automatisch über die Notwendigkeit, ein aktuelles Dokument in Übereinstimmung mit dem Risikoprofil des Kunden anzufordern. Das System umfasst auch eine Kontrolle des Verfallsdatums und sendet eine Benachrichtigung, wenn das Ausweisdokument/der Adressnachweis des Kunden kurz vor dem Verfallsdatum steht.

Die gesammelten Dokumente, Daten und Informationen müssen auch überprüft werden, wenn ein Ereignis eingetreten ist, das die Notwendigkeit einer Aktualisierung der gesammelten Dokumente, Daten und Informationen anzeigt.

Im Rahmen der **laufenden Überwachung der Geschäftsbeziehung** wird die Gesellschaft die während der Geschäftsbeziehung abgeschlossenen Transaktionen so überwachen, dass sie feststellen kann, ob die abzuschließenden Transaktionen mit den zuvor über den Kunden bekannten Informationen übereinstimmen (d.h. mit dem, was der Kunde bei Aufnahme der Geschäftsbeziehung angegeben hat oder was im Laufe der Geschäftsbeziehung bekannt geworden ist).

Das Unternehmen überwacht die Geschäftsbeziehung auch, um Aktivitäten oder Fakten des Kunden festzustellen, die auf kriminelle Aktivitäten, Geldwäsche oder Terrorismusfinanzierung hindeuten oder deren Zusammenhang mit Geldwäsche oder Terrorismusfinanzierung wahrscheinlich ist, einschließlich komplizierter, hochwertiger und ungewöhnlicher Transaktionen und Transaktionsmuster, die keinen vernünftigen oder offensichtlichen wirtschaftlichen oder legitimen Zweck haben oder die für die Besonderheiten des betreffenden Geschäfts untypisch sind. Im Laufe der Geschäftsbeziehung bewertet das Unternehmen ständig die Änderungen in den Aktivitäten des Kunden und bewerten, ob diese Änderungen das mit dem Kunden und der Geschäftsbeziehung verbundene Risikoniveau erhöhen können, was die Anwendung von EDD-Maßnahmen erforderlich macht.

Im Rahmen der laufenden Überwachung der Geschäftsbeziehung wendet das Unternehmen die folgenden Maßnahmen an:

- Screening, d.h. die Überwachung von Transaktionen in Echtzeit;
- die Überwachung, d.h. die spätere Analyse

der Transaktionen. Das Ziel des **Screenings** ist die

Identifizierung:

- verdächtige und ungewöhnliche Transaktionen und Transaktionsmuster;
- Transaktionen, die die angegebenen Schwellenwerte überschreiten;
- Politisch exponierte Personen und Umstände in Bezug auf Sanktionen.

Die Überprüfung der Transaktionen erfolgt automatisch und umfasst die folgenden Maßnahmen:

- Schwellenwerte für die Transaktionen des Kunden, abhängig vom Risikoprofil des Kunden und dem vom Kunden angegebenen geschätzten Transaktionsumsatz;
- die Bewertung von Geldbörsen für virtuelle Währungen, an die die virtuellen Währungen gemäß der Bestellung des Kunden gesendet werden sollen;
- die Bewertung der Geldbörsen für virtuelle Währungen, von denen die virtuelle Währung empfangen wird.

Wenn der Kunde eine Transaktion in Auftrag gibt, die den festgelegten Schwellenwert überschreitet, oder eine Transaktion an eine virtuelle Geldbörse mit hohem Risiko (z. B. Geldbörsen, die mit Betrug, Kriminalität usw. in Verbindung gebracht werden), wird die Transaktion manuell vom Mitarbeiter genehmigt, der vor der Genehmigung die Notwendigkeit zusätzlicher CDD-Maßnahmen prüft (z. B. Anwendung von EDD-Maßnahmen, Abfrage der Quelle und Herkunft der Mittel oder Abfrage zusätzlicher Informationen zur Transaktion).

Bei der **Überwachung von Transaktionen** bewertet der Mitarbeiter die Transaktionen im Hinblick auf die Aufdeckung von Aktivitäten und Transaktionen, die:

- von dem abweichen, was aufgrund der durchgeführten CDD-Maßnahmen, der erbrachten Dienstleistungen, der vom Kunden zur Verfügung gestellten Informationen und anderer Umstände zu erwarten ist (z. B. Überschreiten des geschätzten Transaktionsumsatzes, Senden von virtueller Währung jedes Mal an eine neue Geldbörse für virtuelle Währung, Überschreiten des Transaktionsvolumens);

Wird der vorgenannte Sachverhalt festgestellt, muss der Mitarbeiter die MLRO benachrichtigen und jegliche Transaktion des Kunden aussetzen, bis die MLRO eine entsprechende Entscheidung getroffen hat.

Darüber hinaus überprüft der MLRO die Transaktionen des Unternehmens regelmäßig (mindestens einmal pro Woche), um sicherzustellen, dass:

- die Mitarbeiter des Unternehmens die oben genannten Verpflichtungen ordnungsgemäß erfüllt haben;
- es keine Transaktionen und Transaktionsmuster gibt, die kompliziert, wertvoll und ungewöhnlich sind und die keinen vernünftigen oder offensichtlichen wirtschaftlichen oder legitimen Zweck haben oder für die spezifischen Merkmale untypisch sind.

Das Unternehmen **identifiziert die Quelle[21] und die Herkunft[22] der** für die Transaktion(en) verwendeten **Gelder**, falls erforderlich. Die Notwendigkeit, die Quelle und Herkunft der Gelder zu identifizieren, hängt von den früheren Aktivitäten des Kunden sowie von anderen bekannten Informationen ab. Die Identifizierung der Quelle und Herkunft der in der Transaktion verwendeten Gelder wird in den folgenden Fällen durchgeführt:

- die Transaktionen die von der Gesellschaft festgelegten Grenzen überschreiten;
- die Transaktionen nicht mit den zuvor bekannten Informationen über den Kunden übereinstimmen;
- das Unternehmen will oder sollte es vernünftigerweise für notwendig erachten, um zu beurteilen, ob die Transaktionen mit den zuvor über den Kunden bekannten Informationen übereinstimmen;
- das Unternehmen vermutet, dass die Transaktionen auf kriminelle Aktivitäten, Geldwäsche oder Terrorismusfinanzierung hindeuten oder dass ein Zusammenhang zwischen den Transaktionen und Geldwäsche oder Terrorismusfinanzierung wahrscheinlich ist, einschließlich komplizierter, hochwertiger und ungewöhnlicher Transaktionen und Transaktionsmuster, die keinen vernünftigen oder offensichtlichen wirtschaftlichen oder legitimen Zweck haben oder für die Besonderheiten des betreffenden Geschäfts untypisch sind.

UMSETZUNG VON SANKTIONEN

Bei Inkrafttreten, Änderung oder Beendigung von Sanktionen prüft das Unternehmen, ob der Kunde, sein wirtschaftlicher Eigentümer oder eine Person, die eine Geschäftsbeziehung oder Transaktion mit ihm plant, Gegenstand von Sanktionen ist. Stellt das Unternehmen fest, dass eine Person Gegenstand von Sanktionen ist oder dass die von ihr beabsichtigte oder durchgeführte Transaktion gegen Sanktionen verstößt, wendet das Unternehmen Sanktionen an und informiert den FCIS innerhalb von 3 Stunden darüber.

Verfahren zur Identifizierung des Gegenstands von Sanktionen und einer gegen Sanktionen verstoßenden Transaktion

Das Unternehmen nutzt mindestens die folgenden Quellen (Datenbanken), um die Beziehung des Kunden zu Sanktionen zu überprüfen:

- Eine konsolidierte Liste der EU-Sanktionen;
- Eine konsolidierte Liste der Sanktionen der Vereinten Nationen

UMSETZUNG VON SANKTIONEN

Bei Inkrafttreten, Änderung oder Beendigung von Sanktionen prüft das Unternehmen, ob der Kunde, sein wirtschaftlicher Eigentümer oder eine Person, die eine Geschäftsbeziehung oder Transaktion mit ihm plant, Gegenstand von Sanktionen ist. Stellt das Unternehmen fest, dass eine Person Gegenstand von Sanktionen ist oder dass die von ihr beabsichtigte oder durchgeführte Transaktion gegen Sanktionen verstößt, wendet das Unternehmen Sanktionen an und informiert den FCIS innerhalb von 3 Stunden darüber.

Verfahren zur Identifizierung des Gegenstands von Sanktionen und einer gegen Sanktionen verstoßenden Transaktion

Das Unternehmen nutzt mindestens die folgenden Quellen (Datenbanken), um die Beziehung des Kunden zu Sanktionen zu überprüfen:

- Eine konsolidierte Liste der EU-Sanktionen;
- Eine konsolidierte Liste der Sanktionen der Vereinten Nationen
- Amt für die Kontrolle ausländischer Vermögenswerte (OFAC).

Zusätzlich zu den oben genannten Quellen kann das Unternehmen auf Beschluss des Mitarbeiters, der die CDD-Maßnahmen anwendet, auch andere Quellen nutzen.

[21] **die Quelle der** für die Transaktion verwendeten **Mittel** ist Grund, Erklärung und Grundlage (Rechtsverhältnis und dessen Inhalt), warum die Mittel übertragen wurden

[22] **die Herkunft der** für die Transaktion verwendeten **Mittel** ist die Tätigkeit, durch die die Mittel verdient oder erhalten wurden

Um zu überprüfen, ob die Namen der Personen, die sich aus der Anfrage ergeben, mit den Personen übereinstimmen, die in einer Mitteilung aufgeführt sind, die eine oder mehrere Sanktionen enthält, werden ihre persönlichen Daten verwendet, deren Hauptmerkmale bei einer juristischen Person ihr Name oder ihre Marke, der Registercode oder das Registrierungsdatum und bei einer natürlichen Person ihr Name und ihre persönliche Kennung oder ihr Geburtsdatum sind.

Um festzustellen, ob die in dem betreffenden Rechtsakt oder der Mitteilung genannten Personen mit den Personen übereinstimmen, die durch die Abfrage von Datenbanken identifiziert wurden, muss das Unternehmen die Namen der durch die Abfrage ermittelten Personen auf mögliche Auswirkungen von Faktoren analysieren, die die personenbezogenen Daten verfälschen (z. B. Transkription ausländischer Namen, abweichende Reihenfolge der Wörter, Ersetzung von diakritischen Zeichen oder Doppelbuchstaben usw.).

Das Unternehmen führt die vorgenannten Überprüfungen im Laufe einer bestehenden Geschäftsbeziehung fortlaufend durch. Die Häufigkeit der laufenden Überprüfungen hängt vom Risikoprofil des Kunden ab:

- einmal pro Woche für das Hochrisikoprofil Kunde;
- einmal pro Monat für den Kunden mit mittlerem Risikoprofil;
- einmal pro Quartal für den Kunden mit niedrigem Risikoprofil.

Wenn der Mitarbeiter Zweifel daran hat, dass eine Person Gegenstand von Sanktionen ist, benachrichtigt er unverzüglich die MLRO oder das Vorstandsmitglied. In diesem Fall entscheidet der MLRO oder das Vorstandsmitglied, ob er zusätzliche Daten von der Person erfragt oder einholt oder ob er die FCIS unverzüglich über seinen Verdacht informiert.

Das Unternehmen beschafft sich in erster Linie selbst zusätzliche Informationen über die Person, die eine Geschäftsbeziehung zu ihr unterhält oder eine Transaktion mit ihr durchführt, sowie über die Person, die beabsichtigt, eine Geschäftsbeziehung zu ihr aufzubauen, eine Transaktion mit ihr durchzuführen oder eine Handlung mit ihr vorzunehmen, wobei es Informationen aus einer glaubwürdigen und unabhängigen Quelle bevorzugt. Wenn solche Informationen aus irgendeinem Grund nicht verfügbar sind, fragt das Unternehmen die Person, die eine Geschäftsbeziehung mit ihr unterhält oder eine Transaktion oder Handlung mit ihr durchführt, sowie die Person, die beabsichtigt, eine Geschäftsbeziehung mit ihr aufzubauen, eine Transaktion oder Handlung mit ihr durchzuführen, ob die Informationen aus einer glaubwürdigen und unabhängigen Quelle stammen, und bewertet die Antwort.

Maßnahmen bei der Identifizierung des Sanktionsträgers oder einer Transaktion, die gegen Sanktionen verstößt

Erhält ein Mitarbeiter des Unternehmens Kenntnis davon, dass ein Kunde, der eine Geschäftsbeziehung mit dem Unternehmen unterhält oder eine Transaktion mit dem Unternehmen durchführt, sowie eine Person, die beabsichtigt, eine Geschäftsbeziehung mit dem Unternehmen aufzubauen oder eine Transaktion mit dem Unternehmen durchzuführen, Gegenstand von Sanktionen ist, muss der Mitarbeiter den MLRO oder das Vorstandsmitglied unverzüglich über die Identifizierung des Gegenstands der Sanktionen, die Zweifel daran und die getroffenen Maßnahmen informieren.

Der MLRO oder das Vorstandsmitglied lehnt den Abschluss einer Transaktion oder eines Verfahrens ab, ergreift die im Gesetz über die Verhängung oder Umsetzung der Sanktionen vorgesehenen Maßnahmen und unterrichtet den FCIS unverzüglich über seine Zweifel und die getroffenen Maßnahmen.

Bei der Identifizierung der Person, gegen die Sanktionen verhängt werden, ist es notwendig, die Maßnahmen zu bestimmen, die ergriffen werden, um diese Person zu sanktionieren. Diese Maßnahmen werden in dem Rechtsakt zur Umsetzung des Sanktionen, daher ist es notwendig, die genaue Sanktion zu identifizieren, die gegen die Person verhängt wird, um eine legale und ordnungsgemäße Anwendung der Maßnahmen zu gewährleisten.

ABLEHNUNG DER TRANSAKTION ODER GESCHÄFTSBEZIEHUNG UND IHRE BEENDIGUNG

Dem Unternehmen ist es untersagt, eine Geschäftsbeziehung aufzubauen und die aufgebaute Geschäftsbeziehung oder Transaktion wird beendet (es sei denn, dies ist objektiv unmöglich), wenn:

- das Unternehmen Geldwäsche oder Terrorismusfinanzierung vermutet;
- es dem Unternehmen nicht möglich ist, die CDD-Maßnahmen anzuwenden, weil der Kunde die entsprechenden Daten nicht übermittelt oder sich weigert, sie zu übermitteln, oder die übermittelten Daten keine Gewähr dafür bieten, dass die erhobenen Daten angemessen sind;
- der Kunde, dessen Kapital aus Inhaberaktien oder anderen Inhaberpapieren besteht, die Geschäftsbeziehung aufnehmen möchte;
- der Kunde, bei dem es sich um eine natürliche Person handelt, hinter der eine andere, tatsächlich begünstigte Person steht, die Geschäftsbeziehung aufnehmen möchte (Verdacht, dass eine Person als Fassade benutzt wird);
- das Risikoprofil des Kunden nicht mehr mit der Risikobereitschaft des Unternehmens übereinstimmt (d. h. das Risikoprofil des Kunden ist "verboten").

Im Falle einer Beendigung der Geschäftsbeziehung gemäß diesem Kapitel überträgt das Unternehmen die Vermögenswerte des Kunden innerhalb eines angemessenen Zeitraums, vorzugsweise jedoch spätestens innerhalb eines Monats nach der Beendigung, als Ganzes auf ein Konto, das bei einem Kreditinstitut eröffnet wurde, das seinen Sitz oder seine Niederlassung in einem Vertragsstaat des Europäischen Wirtschaftsraums oder in einem Land hat, in dem Anforderungen gelten, die denen der einschlägigen Richtlinien des Europäischen Parlaments und des Rates entsprechen. In Ausnahmefällen können die Vermögenswerte auf ein anderes Konto als das des Kunden überwiesen oder in bar ausgegeben werden. Unabhängig vom Empfänger der Gelder muss in den Zahlungsangaben zur Übertragung der Vermögenswerte des Kunden mindestens in englischer Sprache angegeben werden, dass die Übertragung im Zusammenhang mit der außerordentlichen Beendigung der Kundenbeziehung steht.

MELDEPFLICHT

Das Unternehmen muss die Transaktion ungeachtet des Transaktionsbetrages aussetzen (außer in den Fällen, in denen dies aufgrund der Art der monetären Operation oder Transaktion, der Art ihrer Ausführung oder anderer Umstände objektiv unmöglich ist) und muss über seinen MLRO dem FCIS über die Aktivität oder die Umstände berichten, die er im Laufe der wirtschaftlichen Aktivitäten feststellt und wobei:

- das Unternehmen hat festgestellt, dass der Kunde eine verdächtige Transaktion durchführt;

- das Unternehmen weiß oder vermutet, dass Vermögenswerte von beliebigem Wert direkt oder indirekt aus kriminellen Aktivitäten oder der Beteiligung an solchen Aktivitäten stammen.

Die Mindestmerkmale verdächtiger Transaktionen sind in den Leitlinien des FCIS (einer der Anhänge dieser Leitlinien) aufgeführt.

Die oben genannten Meldungen müssen vor Abschluss der Transaktion erfolgen, wenn das Unternehmen den Verdacht hat oder weiß, dass Geldwäsche oder Terrorismusfinanzierung oder damit zusammenhängende Straftaten begangen werden und wenn diese Umstände vor Abschluss der Transaktion festgestellt werden.

Wenn sich die Notwendigkeit der oben genannten Meldung ergibt, muss der Mitarbeiter, dem diese Notwendigkeit bekannt wurde, den MLRO unverzüglich darüber informieren.

In jedem Fall (d.h. auch in der Situation, in der eine Aktivität oder ein Umstand nach Abschluss der Transaktion identifiziert wird) **muss die Meldepflicht für die oben genannten Meldungen unverzüglich, spätestens jedoch drei Arbeitsstunden** nach der Identifizierung der Aktivität oder des Umstands oder dem Aufkommen des tatsächlichen Verdachts (d.h. der Situation, in der der Verdacht nicht ausgeräumt werden kann) **erfolgen**.

Meldepflicht für bestimmte Arten von Transaktionen

Die Gesellschaft muss über ihren MLRO spätestens innerhalb von 7 Arbeitstagen nach Feststellung von Devisentransaktionen oder Transaktionen in virtueller Währung Informationen an das FCIS übermitteln, wenn der Tageswert dieser Transaktion(en) 15.000 EUR oder den entsprechenden Betrag in ausländischer oder virtueller Währung erreicht oder überschreitet, unabhängig davon, ob die Transaktion in einem oder mehreren zusammenhängenden Geldgeschäften abgeschlossen wird.

In den oben genannten Fällen müssen die an das FCIS übermittelten Informationen Folgendes umfassen:

- die Daten zur Bestätigung der Identität des Kunden und - falls die Transaktion über einen Vertreter abgewickelt wird - auch die Daten zur Bestätigung der Identität des Vertreters;
- den Betrag der Transaktion;
- die Währung, in der dieTransaktion ausgeführt wurde;
- das Datum der Ausführung der Transaktion;
- die Art und Weise der Durchführung der Währungsoperation;
- das Unternehmen, zu dessen Gunsten die Geldtransaktion durchgeführt wurde (falls möglich);
- andere Daten, die in den entsprechenden FCIS-Anweisungen angegeben sind.

Alle in diesem Kapitel beschriebenen Berichte werden in Übereinstimmung mit den Berichterstattungsrichtlinien des Unternehmens über einen sicheren Kanal übermittelt, der volle Vertraulichkeit gewährleistet (einer der Anhänge dieser Richtlinien).

Dem Unternehmen, einer strukturellen Einheit des Unternehmens, einem Vorstandsmitglied, MLRO und dem Mitarbeiter ist es untersagt, eine Person, ihren wirtschaftlichen Eigentümer, einen Vertreter oder einen Dritten über eine über sie an das FCIS übermittelte Meldung, einen Plan zur Übermittlung einer solchen Meldung oder das Auftreten

der Berichterstattung sowie über eine Anordnung des FCIS oder über die Einleitung eines Strafverfahrens.

AUSBILDUNGSPFLICHT

Das Unternehmen stellt sicher, dass seine Mitarbeiter, seine Auftragnehmer und andere Personen, die auf ähnlicher Basis am Geschäft beteiligt sind und Arbeitsaufgaben ausführen, die für die Verhinderung der Nutzung des Geschäfts des Unternehmens für Geldwäsche oder Terrorismusfinanzierung von Bedeutung sind ("Relevante Personen"), über die entsprechenden Qualifikationen für diese Arbeitsaufgaben verfügen. Wenn eine Relevante Person eingestellt oder engagiert wird, werden die Qualifikationen der Relevanten Person als Teil des Einstellungs-/Ernennungsprozesses überprüft, indem Hintergrundprüfungen durchgeführt werden, die mit einem speziellen Standardformular zur Bewertung der Eignung des Mitarbeiters dokumentiert werden.

In Übereinstimmung mit den für das Unternehmen geltenden Anforderungen zur Sicherstellung der Eignung relevanter Personen stellt das Unternehmen sicher, dass diese Personen fortlaufend angemessen geschult und informiert werden, damit sie die Verpflichtungen des Unternehmens in Übereinstimmung mit den geltenden Rechtsvorschriften erfüllen können. Durch die Schulung wird sichergestellt, dass diese Personen über Kenntnisse im Bereich AML/CFT verfügen, die den Aufgaben und der Funktion der Person angemessen sind. Die Schulung muss in erster Linie Informationen über alle aktuellen Methoden der Geldwäsche und Terrorismusfinanzierung und die damit verbundenen Risiken vermitteln.

Diese Schulung bezieht sich auf relevante Teile des Inhalts der geltenden Regeln und Vorschriften, der Risikobewertung des Unternehmens, der Richtlinien und Verfahren des Unternehmens sowie auf Informationen, die es den relevanten Personen erleichtern sollen, einen Verdacht auf Geldwäsche und Terrorismusfinanzierung zu erkennen. Die Schulung ist auf der Grundlage der durch die Risikobewertung ermittelten Risiken strukturiert.

Der Inhalt und die Häufigkeit der Schulungen werden an die Aufgaben und die Funktion der Person in Bezug auf AML/CFT-Maßnahmen angepasst. Wenn die Richtlinien in irgendeiner Weise aktualisiert oder geändert werden, werden Inhalt und Häufigkeit der Schulung entsprechend angepasst.

Für neue Mitarbeiter umfasst die Schulung eine Überprüfung des Inhalts der geltenden Regeln und Vorschriften, der Risikobewertungspolitik des Unternehmens, dieser Richtlinien und anderer relevanter Verfahren.

Die Mitarbeiter und die Mitglieder des Vorstands werden unter der Leitung des MLRO gemäß dem folgenden Schulungsplan fortlaufend geschult:

- Periodizität: Mindestens einmal jährlich für die Mitglieder des Vorstands. Mindestens einmal pro Jahr für die Mitarbeiter des Unternehmens und die beauftragte Relevante Person.
- Umfang: Überprüfung der geltenden Regeln und Vorschriften, der Richtlinien des Unternehmens und anderer relevanter Verfahren. Spezifische Informationen zu neuen/aktualisierten Merkmalen in den geltenden Regeln und Vorschriften. Bericht und Erfahrungsaustausch über die seit der letzten Schulung überprüften Transaktionen.
  Darüber hinaus werden die Relevanten Personen laufend über neue Trends, Muster und Methoden informiert und erhalten weitere Informationen, die für die Verhinderung von Geldwäsche und Terrorismusfinanzierung relevant sind.

Die durchgeführten Schulungen sind elektronisch zu dokumentieren und mit der Unterschrift der zuständigen Person zu bestätigen. Diese Dokumentation sollte den Inhalt der Schulung, die Namen der Teilnehmer und das Datum der Schulung enthalten.

ERFASSUNG UND SPEICHERUNG VON DATEN, LOGBÜCHER

Das Unternehmen muss über die Person (einschließlich Mitarbeiter, Vorstandsmitglieder und MLRO), die die relevanten Informationen oder Dokumente zuerst erhält, die folgenden Daten registrieren und aufbewahren:

- alle Daten, die im Rahmen der Umsetzung der CDD-Maßnahmen gesammelt wurden;
- Informationen über die Umstände der Ablehnung der Aufnahme der Geschäftsbeziehung durch das Unternehmen;
- die Umstände der Ablehnung der Aufnahme einer Geschäftsbeziehung auf Initiative des Kunden, wenn die Ablehnung mit der Anwendung von CDD-Maßnahmen durch das Unternehmen zusammenhängt;
- Informationen zu allen Vorgängen, die zur Identifizierung der an der Transaktion beteiligten Person oder des wirtschaftlichen Eigentümers des Kunden vorgenommen wurden;
- Informationen, wenn es unmöglich ist, dieCDD -Maßnahmen durchzuführen;
- Informationen über die Umstände der Beendigung der Geschäftsbeziehung im Zusammenhang mit der Unmöglichkeit der Anwendung der CDD-Maßnahmen
- das jeweilige Transaktionsdatum oder den Zeitraum und eine Beschreibung des Inhalts der Transaktion, einschließlich des Transaktionsbetrags, der Währung und der Kontonummer oder einer anderen Kennung (einschließlich des Hashs von Transaktionen in virtuellen Währungen und virtuellen Währungs-Wallets, die mit der Transaktion verbunden sind);
- Informationen, die als Grundlage für die in den Leitlinien festgelegten Berichtspflichten dienen;
- Daten über verdächtige oder ungewöhnliche Transaktionen oder Umstände, die dem FCIS nicht gemeldet wurden (z. B. komplexe oder ungewöhnlich große Transaktionen, Transaktionen, die nach einem ungewöhnlichen Muster durchgeführt werden, und Transaktionen, die keinen offensichtlichen wirtschaftlichen oder rechtmäßigen Zweck haben, Geschäftsbeziehungen oder monetäre Transaktionen mit Kunden aus Drittländern, in denen die Maßnahmen zur Verhinderung von Geldwäsche und/oder Terrorismusfinanzierung unzureichend sind oder nicht den internationalen Standards entsprechen, gemäß den offiziell von internationalen zwischenstaatlichen Organisationen veröffentlichten Informationen).

Einige der oben genannten Daten werden in chronologischer Reihenfolge auf der Grundlage von Dokumenten, die eine monetäre Operation oder Transaktion bestätigen, oder anderen rechtsgültigen Dokumenten im Zusammenhang mit der Ausführung von monetären Operationen oder Transaktionen in das Logbuch (wie unten beschrieben) eingetragen, und zwar unverzüglich, jedoch nicht später als innerhalb von 3 Geschäftstagen nach der Ausführung einer monetären Operation oder Transaktion. Die oben genannten Daten müssen 8 Jahre nach Beendigung der Geschäftsbeziehung oder des Abschlussgeschäfts aufbewahrt werden. Die Daten, die sich auf die Erfüllung der Meldepflicht beziehen, müssen für 5 Jahre nach Erfüllung der Meldepflicht aufbewahrt werden.

Die Korrespondenz einer Geschäftsbeziehung mit dem Kunden muss für 5 Jahre ab dem Datum der Beendigung der Transaktionen oder der Geschäftsbeziehung aufbewahrt werden.

Dokumente und Daten müssen so aufbewahrt werden, dass sie eine umfassende und sofortige Beantwortung der Anfragen des FCIS oder, gemäß den gesetzlichen Bestimmungen, anderer Aufsichtsbehörden, Ermittlungsbehörden oder des Gerichts ermöglichen.

Das Unternehmen setzt alle Regeln des Schutzes personenbezogener Daten in Anwendung der sich aus dem geltenden Recht ergebenden Anforderungen um. Das Unternehmen darf personenbezogene Daten, die bei der Durchführung der CDD erhoben wurden, nur zum Zweck der Verhinderung von Geldwäsche und Terrorismusfinanzierung verarbeiten. Die Daten dürfen nicht zusätzlich in einer Weise verarbeitet werden, die dem Zweck nicht entspricht, z.B. für Marketingzwecke.

Das Unternehmen löscht die auf Vorrat gespeicherten Daten nach Ablauf der Frist, es sei denn, die Gesetzgebung, die den entsprechenden Bereich regelt, sieht ein anderes Verfahren vor. Auf der Grundlage einer Anordnung der zuständigen Aufsichtsbehörde können Daten, die für die Verhinderung, Aufdeckung oder Untersuchung von Geldwäsche oder Terrorismusfinanzierung von Bedeutung sind, für einen längeren Zeitraum aufbewahrt werden, jedoch nicht länger als zwei Jahre nach Ablauf des ersten Zeitraums.

Führen von Meldelogbüchern

Für die Zwecke der Erfüllung der AML-Verpflichtungen führt (vervollständigt) das Unternehmen die folgenden Registrierungslogbücher, die die Geldgeschäfte und Transaktionen widerspiegeln (im Folgenden - Logbücher):

- Logbuch von Kunden, die Transaktionen in virtueller Währung durchführen, unabhängig davon, ob die Transaktionen gelegentlich oder im Rahmen einer Geschäftsbeziehung durchgeführt werden;
- Logbuch der Geldgeschäfte oder Transaktionen, die zwischen dem Kunden und dem Unternehmen durchgeführt wurden, bevor das Unternehmen verpflichtet ist, CDD-Maßnahmen anzuwenden;
- Logbuch der Berichte[23] und verdächtige Geldtransaktionen und Transaktionen;
- Logbuch der Kunden, mit denen Transaktionen oder Geschäftsbeziehungen aufgrund von Verstößen gegen das Verfahren zur Verhinderung von Geldwäsche und/oder Terrorismusfinanzierung verweigert oder abgebrochen w u r d e n .

Das Registrierungslogbuch von Kunden, die Transaktionen in virtueller Währung durchführen, muss Folgendes enthalten:

- Daten, die die Identität des Kunden und seines Vertreters bestätigen (wenn die Geldtransaktion durchgeführt oder die Transaktion durch einen Vertreter abgeschlossen wird): Vor- und Nachname einer natürlichen Person, persönlicher Identifikationscode (Geburtsdatum eines ausländischen Kunden), Staatsangehörigkeit; persönlicher Code, falls ein solcher Code angegeben ist;
- bei Transaktionen mit virtuellen Währungen oder Transaktionen, bei denen es objektiv nicht möglich ist, den Zahlungsempfänger zu identifizieren, andere Informationen, die es ermöglichen, die Adresse der virtuellen Währung zu ermitteln

[23] wie in dem entsprechenden Kapitel dieser Richtlinien beschrieben

die mit der Identität des Besitzers der virtuellen Währung verknüpft sind: Internet Protocol (IP)-Adresse, E-Mail-Adresse, etc;

- Adresse(n) der virtuellen Währung in Bezug auf die Transaktion und den/die Hash(s) der Transaktion;
- Transaktionsmethode: Einzahlung oder Abhebung von virtueller Währung, Umtausch von virtueller Währung in Geld oder umgekehrt, Umtausch von virtueller Währung in andere virtuelle Währung, Umtauschtransaktion von virtueller Währung wurde vermittelt (p2p-Tausch);

Das Registrierungsbuch für Geldgeschäfte oder Transaktionen, die zwischen dem Kunden und dem Unternehmen durchgeführt wurden, bevor das Unternehmen verpflichtet ist, CDD-Maßnahmen anzuwenden, muss Folgendes enthalten:

- Daten, die die Identität des Kunden und seines Vertreters bestätigen (wenn die Geldtransaktion durchgeführt oder die Transaktion durch einen Vertreter abgeschlossen wird): Vor- und Nachname einer natürlichen Person, persönlicher Identifikationscode (Geburtsdatum eines ausländischen Kunden), Staatsangehörigkeit; persönlicher Code, falls ein solcher Code angegeben ist;
- Daten zum Geldgeschäft oder zur Transaktion: das Datum der Transaktion, die Beschreibung der Vermögenswerte, die Gegenstand der Transaktion sind (Bargeld, Immobilien, virtuelle Währung usw.) und deren Wert (Geldbetrag, Währung, in der das Geldgeschäft oder die Transaktion durchgeführt wird, Marktwert der Vermögenswerte usw.);
- Transaktionsmethode: Virtuelle Währung wird in Geld umgetauscht oder umgekehrt, der Kunde hat eine Vorauszahlung für den Kauf von virtueller Währung geleistet, usw.

Das Logbuch zur Registrierung von Berichten, verdächtigen Geldgeschäften und Transaktionen muss in chronologischer Reihenfolge Folgendes enthalten:

- Daten, die die Identität des Kunden und seines Vertreters bestätigen (wenn die Geldtransaktion durchgeführt oder die Transaktion durch einen Vertreter abgeschlossen wird): Vor- und Nachname einer natürlichen Person, persönlicher Identifikationscode (Geburtsdatum eines ausländischen Kunden), Staatsangehörigkeit; persönlicher Code, falls ein solcher Code angegeben ist;
- das vom Innenministerium der Republik Litauen genehmigte Kriterium, nach dem die Geldtransaktion oder das Geschäft des Kunden als verdächtig eingestuft wird, die Transaktion oder das Geschäft erfüllt;
- Art und Weise des Abschlusses einer verdächtigen Geldoperation oder Transaktion;
- Datum und Uhrzeit der verdächtigen monetären Operation oder Transaktion, Charakterisierung der Vermögenswerte, die Gegenstand der Transaktion sind (Bargeld usw.), und ihr Wert (Geldbetrag, Währung, die für die Durchführung der monetären Operation oder Transaktion verwendet wurde, Marktwert des Vermögenswerts);
- die Daten des/der Transaktionsempfänger(s): vollständiger Name und persönliche Identifikationsnummer einer natürlichen Person (bei Ausländern: Geburtsdatum, sofern verfügbar, persönliche Identifikationsnummer oder eine andere eindeutigeSymbolfolge, die der betreffenden Person zur persönlichen Identifikation zugewiesen wurde), und bei juristischen Personen Titel, Rechtsform, eingetragene Adresse und Registrierungsnummer, sofern eine solche zugewiesen wurde;

- Kontaktdaten des Kunden: Telefonnummer(n), E-Mail-Adresse(n), Kontaktperson(en), deren Telefonnummern, E-Mail-Adressen, usw;
- Beschreibung der Vermögenswerte, die der Kunde ab dem Zeitpunkt der Aussetzung der verdächtigen Geldtransaktion oder des verdächtigen Geschäfts nicht mehr kontrollieren oder nutzen kann (Ort und andere Informationen zur Charakterisierung der Vermögenswerte);
- Im Falle einer verdächtigen Geldtransaktion oder einer Transaktion, die nicht ausgesetzt wurde, relevante Gründe;
- Methoden der Kontoführung;
- Andere relevante Details, je nach Entscheidung des Mitarbeiters.

Das Unternehmen nimmt in das Registrierungsbuch der Kunden, deren Transaktionen oder Geschäftsbeziehungen beendet wurden, in chronologischer Reihenfolge Folgendes auf:

- Daten, die die Identität des Kunden und seines Vertreters bestätigen (wenn die Geldtransaktion durchgeführt oder die Transaktion durch einen Vertreter abgeschlossen wird): Vor- und Nachname einer natürlichen Person, persönlicher Identifikationscode (Geburtsdatum eines ausländischen Kunden), Staatsangehörigkeit; persönlicher Code, falls ein solcher Code angegeben ist;
- Daten zum Geldgeschäft oder zur Transaktion: das Datum der Transaktion, die Beschreibung der Vermögenswerte, die Gegenstand der Transaktion sind (Bargeld, Immobilien, virtuelle Währung usw.), und deren Wert (Geldbetrag, Währung, in der das Geldgeschäft oder die Transaktion durchgeführt wird, Marktwert der Vermögenswerte usw.);
- bei Transaktionen mit virtuellen Währungen oder Transaktionen, bei denen es objektiv nicht möglich ist, den Zahlungsempfänger zu identifizieren, andere Informationen, die es ermöglichen, die Adresse der virtuellen Währung mit der Identität des Eigentümers der virtuellen Währung zu verknüpfen: Internet-Protokoll-Adresse (IP), E-Mail-Adresse usw;
- im Falle von Transaktionen mit virtuellen Währungen die Adresse(n) der virtuellen Währung(en), die mit der Transaktion und dem/den Hash(s) der Transaktion verbunden ist/sind;
- die Daten des/der Begünstigten des Kunden: vollständiger Name und persönliche Identifikationsnummer einer natürlichen Person (im Falle eines Ausländers: Geburtsdatum, falls vorhanden, persönliche Identifikationsnummer oder eine andere eindeutige Symbolfolge, die der betreffenden Person zur persönlichen Identifikation zugewiesen wurde), und im Falle einer juristischen Person Titel, Rechtsform, eingetragene Adresse und Registrierungsnummer, falls eine solche zugewiesen wurde;
- Gründe für die Beendigung von Transaktionen oder Geschäftsbeziehungen im Zusammenhang mit Verstößen gegen das Verfahren zur Verhinderung von Geldwäsche und/oder Terrorismusfinanzierung.

Verfahren für das Führen und Verwalten von Fahrtenbüchern

Die Speicherung der Protokolldaten wird von dem Vorstandsmitglied, wenn es sich auf einer Geschäftsreise befindet oder aus anderen triftigen Gründen nicht zur Verfügung steht, von einem anderen Mitarbeiter ausgefüllt und auf einem elektronischen Datenträger aufbewahrt, wie in der besonderen Anordnung des Direktors angegeben, in der der Umfang der Aufgaben und Verantwortlichkeiten festgelegt ist, die einer Person übertragen werden, die als Stellvertreter handelt.

Der Vorstand ernennt einen Mitarbeiter, der die Aufgabe hat, den Schutz der in den Fahrtenbüchern enthaltenen und in einem elektronischen Medium verarbeiteten Daten vor unbefugter Löschung, Veränderung oder Nutzung durch Dritte zu gewährleisten.
Die Details müssen mit einer Software gespeichert werden, die den Export der Details in Microsoft Office Excel, Word oder eine gleichwertige Open-Code-Software ermöglicht, ohne die Integrität der Details zu beeinträchtigen.

Das Führen der Eintragungsbücher wird von einem Vorstandsmitglied überprüft, wenn es sich auf einer Geschäftsreise befindet oder aus anderen triftigen Gründen nicht verfügbar ist, oder von einem anderen verantwortlichen Mitarbeiter, der von der Gesellschaft ernannt wurde, wie in der besonderen Anordnung des Direktors angegeben, in der der Umfang der Aufgaben und Verantwortlichkeiten einer Person festgelegt ist, die als Stellvertreter fungiert.

Den Mitarbeitern der Gesellschaft ist es untersagt, Kunden oder andere Personen darüber zu informieren oder anderweitig wissen zu lassen, dass Informationen über die stattfindenden Geldgeschäfte oder die von einem Kunden durchgeführten Transaktionen oder die daraus resultierenden Ermittlungen an das FCIS weitergegeben werden.

INTERNE KONTROLLE DER UMSETZUNG DER LEITLINIEN

Die Einhaltung der Leitlinien wird intern durch das Vorstandsmitglied oder den vom Vorstand für die Ausübung der entsprechenden Funktionen ernannten Mitarbeiter (im Folgenden in diesem Kapitel - interner Kontrollbeauftragter) kontrolliert. Der Interne Kontrollbeauftragte muss über die erforderlichen Kompetenzen, Instrumente und den Zugang zu den relevanten Informationen in allen Struktureinheiten des Unternehmens verfügen.

Der Interne Kontrollbeauftragte nimmt interne Kontrollfunktionen zumindest in den folgenden Bereichen wahr:

- die Einhaltung der festgelegten Risikobewertungspolitik und Risikobereitschaft durch das Unternehmen;
- Durchführung von CDD-Maßnahmen;
- Umsetzung von Sanktionen;
- die Verpflichtung des Unternehmens zur Ablehnung der Transaktion oder der Geschäftsbeziehung und deren Beendigung;
- die Meldepflicht des Unternehmens an den FCIS;
- die Verpflichtung des Unternehmens zur Schulung in Bezug auf die AML/CFT-Anforderungen;
- die Verpflichtung des Unternehmens zur Sammlung und Aufbewahrung von Daten.

Die genauen Maßnahmen zur Durchführung der internen Kontrolle werden vom Beauftragten für die interne Kontrolle festgelegt und müssen der Größe des Unternehmens sowie der Art, dem Umfang und dem Grad der Komplexität der Tätigkeiten und Dienstleistungen entsprechen. Die internen Kontrollstellen müssen mindestens die oben genannten Prüfungsbereiche berücksichtigen. Die Maßnahmen der internen Kontrolle werden zu dem vom Beauftragten für die interne Kontrolle festgelegten Zeitpunkt und in der von ihm festgelegten Häufigkeit durchgeführt, mindestens jedoch einmal im Monat, sofern die Art der Maßnahme nicht ausdrücklich etwas anderes vorsieht.

Der Internal Control Officer darf anderen Mitarbeitern oder Dritten (z. B. Beratern, Wirtschaftsprüfern usw.) nur mit vorheriger Zustimmung des Vorstands Zugang zu den Internen Kontrolldaten gewähren. Die Personen, die Zugang zu den Internen Kontrolldaten haben, dürfen diese nicht ohne vorherige Zustimmung des Vorstands an Dritte weitergeben.

Die Internen Kontrolldaten werden in chronologischer Reihenfolge und in einem Format gespeichert, das es ermöglicht, diese zu analysieren und mit anderen relevanten Daten zu verknüpfen.

Der Interne Kontrollbeauftragte legt dem Vorstand mindestens vierteljährlich und der Hauptversammlung der Gesellschaft mindestens einmal jährlich einen Bericht über die interne Kontrolle vor. Der Bericht über die interne Kontrolle enthält mindestens die folgenden Angaben:

- Zeitraum der Ausübung der internen Kontrolle;
- Name und Position der Person, die die interne Kontrolle durchführt;
- Beschreibung der durchgeführten internen Kontrollmaßnahmen;
- die Ergebnisse der internen Kontrolle;
- allgemeine Schlussfolgerungen aus der ausgeübten internen Kontrolle;
- festgestellte Mängel, die in der Periode der Ausübung der internen Kontrolle beseitigt wurden;
- festgestellte Mängel, die am Ende des Zeitraums, in dem die interne Kontrolle ausgeübt wurde, nicht behoben waren;
- Maßnahmen, die zur Beseitigung der festgestellten Mängel durchgeführt werden müssen.

Der Vorstand prüft den vorgelegten Bericht über die interne Kontrolle und fasst einen Beschluss darüber. Der Beauftragte für die interne Kontrolle wird über den Inhalt eines solchen Beschlusses in einem Format informiert, das schriftlich wiedergegeben werden kann. Aus diesem Grund ist der Vorstand dazu verpflichtet:

- analysieren Sie die Ergebnisse der durchgeführten internen Kontrolle;
- Maßnahmen zur Beseitigung von Mängeln zu ergreifen.

Das Unternehmen muss das interne Kontrollverfahren mindestens jährlich und in den folgenden Fällen überprüfen und gegebenenfalls aktualisieren:

- nach der Veröffentlichung der Ergebnisse einer EU-weiten Risikobewertung der Geldwäsche und Terrorismusfinanzierung durch die Europäische Kommission (verfügbar auf der Website der Europäischen Kommission http://ec.europa.eu);
- nach der Veröffentlichung der Ergebnisse der nationalen Risikobewertung für Geldwäsche und Terrorismusfinanzierung (veröffentlicht im Abschnitt "Nationale Risikobewertung für Geldwäsche und Terrorismusfinanzierung" des Abschnitts "Verhinderung von Geldwäsche" auf der Website www.fntt.lt);
- nach Erhalt einer Anweisung des FCIS zur Verstärkung der geltenden internen Kontrollverfahren;

- bei bedeutenden Ereignissen oder Änderungen in der Verwaltung und im Betrieb des Betreibers der Verwahrstelle für virtuelles Geld und des Betreibers der virtuellen Währungsbörse.

Risikobewertung und Risikobereitschaft

Das Ziel der Umsetzung interner Kontrollmaßnahmen zur Einhaltung der festgelegten Risikobewertungspolitik des Unternehmens (einschließlich der festgelegten Risikobereitschaft) ist die Prüfung der folgenden Umstände:

- Das Unternehmen führt einen risikobasierten Ansatz ein und wendet ihn an, wenn es Dienstleistungen für Kunden erbringt (z. B. CDD-Maßnahmen, die entsprechend dem Risikoniveau umgesetzt werden);
- Das Unternehmen hat die Faktoren ermittelt, die sich auf die Entstehung von ML/TF-Risiken auswirken, und die ermittelten Faktoren sind relevant;
- Das Unternehmen hat die ML/TF aller Dienstleistungen, die das Unternehmen erbringt, ermittelt und bewertet;
- Das Unternehmen hat das Risikoprofil des Kunden zusammengestellt, bevor es Transaktionen durchführt oder eine Geschäftsbeziehung aufnimmt;
- Das Unternehmen aktualisiert das Risikoprofil des Kunden regelmäßig;
- Das Unternehmen folgt der festgelegten Risikobereitschaft;
- Das Unternehmen führt Aufzeichnungen über alle Vorfälle in Übereinstimmung mit den festgelegten Richtlinien zur Risikobewertung;
- Die Risikobewertungspolitik wurde im letzten Jahr überprüft und es gibt keine Informationen darüber, dass die MLRO eine frühere Überprüfung erforderlich gemacht hätte.

Umsetzung von Maßnahmen zur Sorgfaltspflicht gegenüber Kunden

Das Ziel der Umsetzung interner Kontrollmaßnahmen für die Einhaltung der CDD-Maßnahmen des Unternehmens ist eine Prüfung der folgenden Umstände:

- das Unternehmen die in den Richtlinien vorgeschriebenen CDD-Maßnahmen auf alle relevanten Kunden anwendet;
- das Unternehmen bei der Anwendung von CDD-Maßnahmen die richtigen Dokumente und Informationen sammelt;
- das Unternehmen die bei der Anwendung von CDD-Maßnahmen erhobenen Daten und Dokumente ordnungsgemäß überprüft;
- das Unternehmen wendet die entsprechende Stufe von CDD-Maßnahmen an (z. B. EDD-Maßnahmen usw.);
- das Unternehmen wendet angemessene EDD-Maßnahmen für bestimmte Kunden an (z. B. PEP, Hochrisikoländer usw.);
- das Unternehmen führt die Identifizierung der Kunden gemäß den festgelegten Verfahren durch;
- das Unternehmen den/die Vertreter des Kunden ordnungsgemäß identifiziert;

- das Unternehmen den Zweck und die Art der Geschäftsbeziehung oder Transaktion ordnungsgemäß angibt;
- das Unternehmen die Geschäftsbeziehungen mit Kunden ordnungsgemäß überwacht.

Bei der Anwendung der EDD-Maßnahmen in Bezug auf die natürlichen Personen/juristischen Personen, die in den von der Europäischen Kommission festgelegten Hochrisiko-Drittländern ansässig sind, muss das Company:

- zusätzliche Informationen über den Kunden und BO zu erhalten;
- zusätzliche Informationen über die beabsichtigte Art der Geschäftsbeziehung einholen;
- Informationen über die Herkunft der Mittel und das Vermögen des Kunden und BO;
- Informationen über die Gründe für die beabsichtigten oder abgeschlossenen Transaktionen zu erhalten;
- die Genehmigung des Senior Managers zur Aufnahme von Geschäftsbeziehungen mit diesen Kunden oder die Zustimmung zur Fortsetzung von Geschäftsbeziehungen mit diesen Kunden einholen
- EDD durchführen, indem Sie die Anzahl und den Zeitpunkt der Kontrollen erhöhen und die Arten von Transaktionen auswählen, die weitere Untersuchungen erfordern;
- sicherstellen, dass die erste Zahlung eines Kunden von einem Konto bei einem Kreditinstitut getätigt wird, das in einem EU-Mitgliedstaat oder in einem Drittland ansässig ist, das gleichwertige Anforderungen wie das Gesetz stellt und unter der Aufsicht der zuständigen Behörden steht.

Derzeit sind die von der Europäischen Kommission festgelegten Hochrisiko-Drittländer in der Delegierten Verordnung Nr. 2016/1675 der Kommission vom 14. Juli 2016 zur Ergänzung der Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates durch die Bestimmung von Hochrisiko-Drittländern mit strategischen Mängeln aufgeführt und durch die folgenden Verordnungen geändert:

Delegierte Verordnung Nr. 2018/105 der Kommission vom 27. Oktober 2017 zur Änderung der Delegierten Verordnung (EU) 2016/1675 in Bezug auf die Aufnahme Äthiopiens in die Liste der Hochrisiko-Drittländer in der Tabelle unter Punkt I des Anhangs;

Delegierte Verordnung Nr. 2018/212 der Kommission vom 13. Dezember 2017 zur Änderung der Delegierten Verordnung (EU) 2016/1675 zur Ergänzung der Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates hinsichtlich der Aufnahme von Sri Lanka, Trinidad und Tobago und Tunesien in die Tabelle unter Punkt I des Anhangs;

Delegierte Verordnung Nr. 2018/1467 der Kommission vom 27. Juli 2018 zur Änderung der Delegierten Verordnung (EU) 2016/1675 zur Ergänzung der Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates hinsichtlich der Aufnahme Pakistans in die Tabelle unter Punkt I des Anhangs.

Basierend auf den Ergebnissen der nationalen Risikobewertung für Geldwäsche und Terrorismusfinanzierung muss das Unternehmen, wenn in der Republik Litauen ein hohes ML/TF-Risiko in Bezug auf die von der Europäischen Kommission festgelegten Hochrisiko-Drittländer festgestellt wird, eine oder mehrere zusätzliche Maßnahmen ergreifen, um das

ML/TF-Risiko wirksam zu verringern, wenn es internationale Korrespondenzbeziehungen mit in diesen Ländern ansässigen Finanzinstituten eingeht oder unterhält:

- zusätzliche Maßnahmen zur verstärkten Überwachung von Geschäftsbeziehungen anwenden, um das Risiko von ML/TF zu verringern;
- die Meldung von verdächtigen Geldgeschäften und Transaktionen zu verschärfen;
- die Geschäftsbeziehungen oder Transaktionen mit natürlichen oder juristischen Personen einschränken, die in von der Europäischen Kommission identifizierten Hochrisiko-Drittländern ansässig sind.

Wenn diese zusätzlichen Maßnahmen nicht ausreichen, um das Risiko zu verringern, sollte das Unternehmen die Aufnahme oder Beendigung von internationalen Korrespondenzbeziehungen mit diesen Finanzinstituten ablehnen.

Derzeit sind die Hochrisiko-Drittländer, die auf der FATF-Liste der Staaten stehen, die schwerwiegende Mängel im Bereich der Prävention von Geldwäsche und Terrorismusfinanzierung und der Bekämpfung dieser Verbrechen aufweisen, zu finden: http://www.fatf-gafi.org/countries/#high-risk. Da sich die Liste jedoch ändert, muss das Unternehmen überwachen, ob die Liste nicht geändert wurde und gegebenenfalls geeignete Maßnahmen ergreifen.

Bei der Anwendung der EDD-Maßnahmen in Bezug auf natürliche Personen/juristische Personen, die in Hochrisiko-Drittländern ansässig sind, die auf der FATF-Liste der Staaten stehen, die schwerwiegende Mängel im Bereich der Prävention von Geldwäsche und Terrorismusfinanzierung und der Bekämpfung dieser Verbrechen aufweisen, muss das Unternehmen:

- eine Genehmigung des Senior Managers zum Abschluss einer Geschäftsbeziehung mit diesen Kunden oder zur Fortsetzung der Geschäftsbeziehung mit diesen Kunden erhalten;
- geeignete Maßnahmen zu ergreifen, um die Quelle des Vermögens und die Quelle der Gelder im Zusammenhang mit der Geschäftsbeziehung oder Transaktion zu ermitteln;
- eine verstärkte laufende Überwachung der Geschäftsbeziehung mit diesen Kunden durchzuführen.

Bei der Bestimmung der Kunden, die ein hohes ML/TF-Risiko darstellen, muss das Unternehmen eine Risikobewertung der Geschäftsbeziehungen durchführen. Unter Berücksichtigung der Ergebnisse zumindest der Risikobewertung des Unternehmens, der nationalen Risikobewertung und der supranationalen Risikobewertung sollte das Unternehmen bei der Bewertung der ML/TF-Risiken, die potenziell von den folgenden Personen und Einrichtungen ausgehen, besondere Sorgfalt walten lassen:

- Händler von Waren, die im Rahmen ihrer Geschäftstätigkeit in der Regel erhebliche Barzahlungen leisten oder erhalten;
- Unternehmen, die in den Teilsektoren des Finanzsektors tätig sind oder Produkte anbieten, die mit Bargeld zu tun haben (z.B. Wechselstuben, Geldtransfers, bestimmte E-Geld-Produkte);
- bestimmte FinTech-Unternehmen (d.h. technologiegestützte und -unterstützte Finanzdienstleistungen), insbesondere mit einer hohen Anzahl von Geschäftsbeziehungen ohne persönliche Kontakte;

- Betreibern von Börsenplattformen für virtuelle Währungen und/oder Anbietern von verwahrten Geldbörsen;
- Andere Verpflichtete, insbesondere Anbieter von Gabling-Diensten und/oder Lotterien und Spielautomaten;
- Non-Profit-Organisationen;
- Andere.

Darüber hinaus sollte das Unternehmen bei der Bewertung der ML/TF-Risiken, die potenziell von den Kunden ausgehen, insbesondere Folgendes berücksichtigen:

- die Kunden, für die zuvor eine STR eingereicht wurde;
- die Kunden, die in der Vergangenheit auf den internationalen oder nationalen Finanzsanktionslisten standen und andere;
- die Kunden, die Gegenstand eines Ersuchens oder einer Information sind, die von der FIU, anderen Ermittlungsbehörden, der Staatsanwaltschaft oder einem Gericht in Bezug auf Informationen über einen Kunden oder dessen Geldgeschäfte oder Transaktionen erhalten wurden, die mit ML/TF oder anderen kriminellen Aktivitäten in Verbindung stehen könnten.

Bei der Feststellung, ob ein erhöhtes ML/TF-Risiko besteht, muss das Unternehmen mindestens die folgenden Faktoren bewerten:

- Eigenschaften des Kunden:
- die Geschäftsbeziehung mit dem Kunden unter ungewöhnlichen Umständen geführt wird, die keinen offensichtlichen wirtschaftlichen oder sichtbaren rechtmäßigen Zweck haben;
- der Wohnsitz des Kunden sich in einem Drittland befindet;
- die juristischen Personen und Einrichtungen ohne Rechtspersönlichkeit sind mit der Tätigkeit der individuellen Immobilienverwaltung befasst;
- das Unternehmen hat formelle Aktionäre, die für eine andere Person handeln, oder hält Inhaberaktien;
- Bargeld ist in diesem Geschäft vorherrschend;
- die Eigenkapitalstruktur der juristischen Person ist offensichtlich ungewöhnlich oder übermäßig komplex in Anbetracht der Art der Aktivitäten der juristischen Person,
- Merkmale des Produkts, der Dienstleistung, der Transaktion oder des Servicekanals:
- Private Banking;
- Produkt oder Transaktion kann günstige Bedingungen für Anonymität schaffen;
- Geschäftsbeziehungen oder gelegentliche Transaktionen werden ohne physische Anwesenheit abgeschlossen oder durchgeführt;
- Zahlungen von unbekannten oder unbeteiligten Dritten erhalten werden;
- Das Produkt oder die Geschäftspraktiken, einschließlich des Mechanismus der Dienstleistungserbringung, sind neu, ebenso wie die Verwendung neuer oder sich entwickelnder Technologien, die bei der Arbeit mit neuen und früheren Produkten zum Einsatz kommen,
- Eigenschaften des Territoriums:
- gemäß den Daten von Berichten oder ähnlichen Dokumenten der FATF oder einer anderen ähnlichen regionalen Organisation erhebliche Verstöße im System der Geldwäschebekämpfung gegen die internationalen Anforderungen festwerden;

- der Staat unterliegt Sanktionen, einem Embargo oder ähnlichen Maßnahmen, die z.B. von der EU oder den Vereinten Nationen verhängt wurden;
- der Staat terroristische Aktivitäten finanziert oder unterstützt oder terroristische Organisationen, die auf den Listen internationaler Organisationen stehen, auf dem Gebiet des Staates operieren.

Umsetzung von Sanktionen

Das Ziel der Umsetzung interner Kontrollmaßnahmen zur Einhaltung der Sanktionen durch das Unternehmen ist eine Prüfung der folgenden Umstände:

- das Unternehmen wendet ein Verfahren zur Identifizierung eines Sanktionsträgers oder einer Transaktion an, die gegen Sanktionen verstößt;
- das Unternehmen Maßnahmen ergreift, wenn es einen Gegenstand von Sanktionen oder eine Transaktion identifiziert, die Sanktionen verletzt.

Verpflichtung zur Ablehnung von Transaktionen oder Geschäftsbeziehungen und deren Beendigung

Ziel der Umsetzung interner Kontrollmaßnahmen zur Einhaltung der Verpflichtung des Unternehmens zur Ablehnung der Transaktion oder Geschäftsbeziehung und deren Beendigung ist eine Prüfung der folgenden Umstände:

- das Unternehmen lehnt eine Transaktion oder Geschäftsbeziehung ab, wenn sie gemäß den Richtlinien obligatorisch ist;
- das Unternehmen verweigert oder beendet eine Transaktion oder Geschäftsbeziehung, wenn dies gemäß den Richtlinien zwingend erforderlich ist.

Meldepflicht

Das Ziel der Implementierung interner Kontrollmaßnahmen zur Einhaltung der Berichtspflicht durch das Unternehmen ist die Prüfung der folgenden Umstände:

- das Unternehmen sendet Berichte und Informationen an den FCIS, wenn dies in den Richtlinien (einschließlich der entsprechenden FCIS-Richtlinien) vorgeschrieben ist;
- die an FCIS gesendeten Berichte in Übereinstimmung mit den Richtlinien von FCIS ausgefüllt werden.

Verpflichtung zur Ausbildung

Das Ziel der Implementierung interner Kontrollmaßnahmen zur Einhaltung der Schulungspflicht im Bereich AML/CTF durch das Unternehmen ist eine Prüfung der folgenden Umstände:

- alle Mitarbeiter (einschl. MLRO und Vorstandsmitglieder) über entsprechende Schulungen verfügen;
- jeder Mitarbeiter (inkl. MLRO und Vorstandsmitglieder) in den letzten 360 Tagen geschult wurde.

Pflicht zur Sammlung und Aufbewahrung von Daten

Das Ziel der Implementierung interner Kontrollmaßnahmen für die Einhaltung der Verpflichtung zur Datenerfassung und -aufbewahrung durch das Unternehmen ist eine Prüfung der folgenden Umstände:

- alle Daten, die in Übereinstimmung mit den Richtlinien gespeichert werden sollen (im Folgenden in diesem Kapitel - die gespeicherten Daten), ordnungsgemäß in chronologischer Reihenfolge und in einem Format gespeichert wurden, das es ermöglicht, diese zu analysieren und die gespeicherten Daten mit anderen relevanten Daten zu verknüpfen;
- nur Mitarbeiter (einschließlich MLRO und Vorstandsmitglieder) oder autorisierte Dritte haben Zugang zu den gespeicherten Daten;
- alle relevanten Logbücher in Übereinstimmung mit den Richtlinien geführt werden;
- die gespeicherten Daten in elektronischem Format gesichert sind;
- die gespeicherten Daten in anderen Formaten (z. B. auf Papier) eine Sicherung in elektronischem Format haben;
- werden die gespeicherten Daten in Übereinstimmung mit den Richtlinien unwiderruflich gelöscht.

ANHÄNGE

Anhang Titel	Beschreibung des Dokuments
Politik der Risikobewertung	Legt die Grundsätze für das Risikomanagement des Unternehmens (einschließlich Risikobewertung und Risikofaktoren) in Bezug auf Geldwäsche und Risiken der Terrorismusfinanzierung.
Profile der Kunden	Tabelle für die Risikobewertung der Kunden und die Dokumentation dieser Bewertung. Enthält Risikofaktoren für jede Risikokategorie.
Onboarding-Verfahren für Kunden	Legt die Anweisungen für das Onboarding des Kunden fest, die im Rahmen der Umsetzung von CDD-Maßnahmen verwendet werden
Fragebögen	Bei der Durchführung von CDD-Maßnahmen (einschließlich der Anwendung von EDD-Maßnahmen, SoW/SoF-Anfragen usw.) wird eine bestimmte Anzahl von Informationen verlangt.
Liste der Quellen	Enthält eine nicht erschöpfende Liste von Ressourcen, die für die Umsetzung von CDD-Maßnahmen verwendet werden können.
Liste der Kriterien für Geldwäsche und Identifizierung verdächtiger Geldgeschäfte oder Transaktionen	Anweisungen und Beispiele für Transaktionen und andere Umstände, die aus Sicht von ML/TF als verdächtig gelten.
Die Liste der Mitarbeiter und ihre Verantwortlichkeiten	Die Liste der Mitarbeiter mit ihren Verbindlichkeiten innerhalb der angegebenen Richtlinien
Logbücher	Die Tabelle ist für die Führung der Logbücher zu verwenden.
MLRO Berichtsformular	Das Berichtsformular, das die MLRO vierteljährlich dem Vorstand vorlegt
Richtlinien zum Ausfüllen der Formulare für die Übermittlung von Informationen an FCIS	FCIS-Leitfaden zum Ausfüllen der entsprechenden Formulare und Formulare selbst.

Aussetzung verdächtiger Geldtransaktionen oder Transaktionen und Übermittlung von Informationen über verdächtige Geldtransaktionen oder Transaktionen an den FCIS	Die entsprechenden FCIS-Richtlinien.
Technische Voraussetzungen für die Kundenidentifizierung per Live-Videoübertragung	FCIS-Leitlinien zu den relevanten technischen Anforderungen
Schulungsprotokoll	Entwurf eines Dokuments, das für jede von der Gesellschaft durchgeführte Schulung der relevanten Personen (einschließlich der Einweisung in die Richtlinien) ausgefüllt werden muss.
Beschluss zur Genehmigung der Leitlinien	Der Entwurf des Beschlusses des Senior Managers des Unternehmens zur Genehmigung dieser Richtlinien.

VERSIONSKONTROLLTABELLE

Version	**Datum der Genehmigung**	**Änderungen Beschreibung**
1.0	tt.mm.jjjj	Erste Ausgabe
1.1	28.03.2023	Aktualisierte Version
1.2	11.07.2023	Aktualisierte Version
2.0	07.08.2023	Zweite Ausgabe
2.1	06.12.2023	Aktualisierte Version
2.2	18.03.2024	Aktualisierte Version

Mariana Achim
18.03.2024