ROX PAY S.R.L.
POLITIK ZUR PRÄVENTION UND BEKÄMPFUNG VON GELDWÄSCHE UND TERRORISMUSFINANZIERUNG

1 - ÜBERSICHT

1.1 – WICHTIGSTE VORSCHRIFTEN UND LEITLINIEN

In diesem Dokument werden die Richtlinien von Rox Pay S.r.l. zur Bekämpfung von Geldwäsche, Terrorismusfinanzierung und Verstößen gegen restriktive Maßnahmen dargelegt[1]und gilt für Rox Pay S.r.l. und seine Operationen.

Normen sind als ergänzend und anwendbar zu betrachten, da sie nicht im Widerspruch zu den von den örtlichen Behörden erlassenen Bestimmungen stehen.

1.2 – EMPFÄNGER UND METHODEN DER UMSETZUNG

Die Richtlinie gilt für Rox Pay S.r.l.

2 – ALLGEMEINE GRUNDSÄTZE

2.1 AML-CFT-REGULIERUNGSRAHMEN

Das Waschen von Erträgen aus illegalen und kriminellen Aktivitäten ist eine der schwerwiegendsten Formen der Kriminalität auf den Finanzmärkten und ein Bereich von besonderem Interesse für organisierte kriminelle Aktivitäten.

Geldwäsche hat erhebliche negative Auswirkungen auf die gesamte Wirtschaft: Die Reinvestition illegaler Erlöse in legale Aktivitäten sowie Absprachen zwischen Einzelpersonen oder Finanzinstituten und kriminellen Organisationen wirken sich tiefgreifend auf die Marktmechanismen aus, untergraben die Effizienz und Fairness finanzieller Aktivitäten und wirken sich schwächend auf die Wirtschaft aus. Die Finanzierung terroristischer Aktivitäten kann die Verwendung rechtmäßiger und/oder kriminell erzielter Erträge beinhalten.

Der sich verändernde Charakter von Geldwäsche und Terrorismusfinanzierung, der auch durch die kontinuierliche Weiterentwicklung der Technologie begünstigt wird, erfordert eine ständige Anpassung der Präventions- und Gegenmaßnahmen.

Der Regulierungsrahmen zur Bekämpfung von Geldwäsche (AML) und Terrorismusfinanzierung (CFT) basiert auf einem umfassenden Satz nationaler, EU- und internationaler Regulierungsquellen.

Auf internationaler Ebene leistete die Financial Action Task Force (FATF), das führende internationale Gremium im Kampf gegen Geldwäsche, Terrorismusfinanzierung und die Verbreitung von Massenvernichtungswaffen, einen wichtigen Beitrag zur Regulierungsharmonisierung.

1 Wie in den EBA-Leitlinien (EBA/GL/2024/14) definiert: „Die restriktiven Maßnahmen der Union im Sinne von Artikel 2 Punkt (1) der Richtlinie (EU) 2024/1226 und die von den Mitgliedstaaten im Einklang mit ihrer nationalen Rechtsordnung erlassenen nationalen restriktiven Maßnahmen (soweit sie für Finanzinstitute gelten).

In Erfüllung ihrer Aufgaben hat die FATF eine Reihe internationaler Standards, die „40 Empfehlungen", festgelegt, zu denen im Jahr 2001 weitere 9 Sonderempfehlungen zur Bekämpfung der internationalen Terrorismusfinanzierung hinzugefügt wurden. Das Thema wurde im Februar 2012 mit der Verabschiedung der Internationalen Standards zur Bekämpfung von Geldwäsche und Terrorismus- und Proliferationsfinanzierung vollständig überarbeitet und anschließend in den oben genannten „40 Empfehlungen" zusammengefasst.

Im Rahmen des Kampfes gegen die Verbreitung von Massenvernichtungswaffen haben die Vereinten Nationen eine Reihe von Maßnahmen zur Bekämpfung der Finanzierung von Proliferationsprogrammen vorbereitet, einschließlich des Verbots, an solchen Aktivitäten beteiligte Personen zu unterstützen oder zu finanzieren.

Bei der Umsetzung der im Rahmen der Vereinten Nationen angenommenen Resolutionen hat die Europäische Union eine Reihe von Bestimmungen erlassen, um restriktive Maßnahmen wie das Einfrieren von Geldern und wirtschaftlichen Ressourcen von Personen oder Organisationen umzusetzen, die an der Entwicklung proliferationsrelevanter Aktivitäten von Massenvernichtungswaffen beteiligt sind.

Die FATF hat Richtlinien zur Umsetzung der von den Vereinten Nationen beschlossenen Finanzsanktionen entwickelt.

Im Einklang mit den Resolutionen des Sicherheitsrats der Vereinten Nationen wurden kürzlich spezifische Maßnahmen zur Bekämpfung der Verbreitung von Massenvernichtungswaffen in die Empfehlungen aufgenommen.

EU-Richtlinien zur Verhinderung der Nutzung des Finanzsystems zur Geldwäsche und Terrorismusfinanzierung sind in der EU-Richtlinie 2015/849 enthalten[2]des Europäischen Parlaments und des Rates vom 20. Mai 2015 (Vierte Geldwäscherichtlinie), geändert durch die EU-Richtlinie 2018/843 (Fünfte Geldwäscherichtlinie) sowie in den jeweils von der EU – Europäische Union und der EBA – Europäische Bankenaufsichtsbehörde herausgegebenen Verordnungen und Leitlinien.

Auf nationaler Ebene wird die Prävention und Bekämpfung von Geldwäsche und Terrorismusfinanzierung durch folgende Primärgesetze geregelt:

- **Italienisches Gesetzesdekret Nr. 109 vom 22. Juni 2007 und nachfolgende Änderungen und Ergänzungen, die „Bestimmungen zur Verhinderung, Bekämpfung und Unterdrückung der Finanzierung des Terrorismus und der Aktivitäten von Ländern, die den Frieden und die internationale Sicherheit bedrohen", zur Umsetzung der Richtlinie 2015/849 in der durch die EU-Richtlinie 2018/843 geänderten Fassung festlegen;**
- **Italienisches Gesetzesdekret Nr. 231 vom 21. November 2007 und nachfolgende Änderungen und Ergänzungen zur Umsetzung der Richtlinie 2015/849/EU, mit der die Richtlinien 2009/138/EG und 2013/36/EU geändert werden, geändert durch die Richtlinie 2018/843/EU zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung (im Folgenden auch das Dekret).**

2 EU-Richtlinie 2024/1640 des Europäischen Parlaments und des Rates vom 31.05.2024 über die von den Mitgliedstaaten einzurichtenden Verfahren zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche oder der Terrorismusfinanzierung, umzusetzen bis zum 10. Juli 2027, ändert die EU-Richtlinie 2019/1937 und hebt die EU-Richtlinie 2015/849 auf.

Schließlich gibt es auch Sekundärgesetze auf nationaler Ebene, die von der Bank von Italien erlassen wurden
und der Financial Information Unit („FIU") und ist in den folgenden Regulierungsquellen enthalten:

- **Bestimmung vom 26. März 2019 zur Festlegung der Durchführungsbestimmungen zu Organisation, Verfahren und internen Kontrollen zur Verhinderung des Einsatzes von Finanzintermediären und anderen Unternehmen zum Zwecke der Geldwäsche und Terrorismusfinanzierung, geändert durch die Bestimmung der Bank von Italien vom 1. August 2023;**
- **Bestimmung vom 28. März 2019 zur Festlegung von Anweisungen zur objektiven Kommunikation;**
- **Bestimmung vom 30. Juli 2019 zur Festlegung der Durchführungsbestimmungen zur Sorgfaltspflicht gegenüber Kunden, geändert durch die Bestimmung der Bank von Italien vom 13. Juni 2023;**
- **Bestimmung vom 24. März 2020 zur Festlegung von Durchführungsbestimmungen für die Speicherung und Verfügbarkeit von Dokumenten, Daten und Informationen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung;**
- **Bestimmung vom 25. August 2020 zur Festlegung von Bestimmungen für die Übermittlung aggregierter AML-Berichte;**
- **Bestimmung vom 12. Mai 2023 über Anomalieindikatoren für Vermittler zur Erleichterung der Identifizierung verdächtiger Transaktionen, gültig ab 1. Januar 2024.**

Rox Pay S.r.l. (im Folgenden „das Unternehmen") setzt die oben genannten Vorschriften in seinen internen Regulierungsdokumenten um.

Auf allgemeiner Ebene hat das Unternehmen diese „Richtlinie zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung" (im Folgenden „Richtlinie") als Ausdruck seines Engagements zur Bekämpfung der oben genannten kriminellen Phänomene auf internationaler Ebene angenommen und dabei besonderes Augenmerk auf den Kontrast gelegt, in dem Bewusstsein, dass das Streben nach Rentabilität und Effizienz mit der kontinuierlichen und wirksamen Überwachung der Integrität der Unternehmensstrukturen verbunden sein muss.

Die im Unternehmen angewandte Richtlinie beschreibt die von Rox Pay S.r.l. angewandte Richtlinie. in Übereinstimmung mit den Regeln und Grundsätzen, die durch nationale und EU-Vorschriften vorgegeben sind, in Übereinstimmung mit den relevanten internationalen Standards und wird gemeinsam mit den internen Verfahren zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung, dem Ethikkodex und internen Verfahren zur Umsetzung der geltenden lokalen primären und sekundären Rechtsvorschriften umgesetzt, die Prozesse, Rollen und Verantwortlichkeiten festlegen.

Die aktuelle Richtlinie wurde vom Vorstand des Unternehmens genehmigt.

Die AML- und CFT-Richtlinien werden von Rox Pay S.r.l. angewendet. im Einklang mit den geltenden Gesetzen.

Das Unternehmen verpflichtet sich zur Einhaltung dieses Regulierungsrahmens sowie aller von der Banca d'Italia erlassenen Durchführungsbestimmungen zur Sorgfaltspflicht gegenüber Kunden, Daten- und Informationsspeicherung, Organisation, Verfahren, Kontrollen und verstärkten Kontrollen gegen die Finanzierung von Programmen zur Verbreitung von Massenvernichtungswaffen.

Das Unternehmen setzt sich voll und ganz dafür ein, dass die Betriebsorganisation und das Kontrollsystem vollständig, angemessen, funktionsfähig und zuverlässig sind, um die strategische Überwachung zu gewährleisten und das Unternehmen vor Duldung oder Beimischung von Formen der Rechtswidrigkeit zu schützen, die seinen Ruf schädigen und seine Stabilität beeinträchtigen können.

Aus diesen Gründen ist Rox Pay S.r.l. hat Organisations- und Verhaltensregeln sowie Überwachungs- und Kontrollsysteme eingeführt, die darauf abzielen, die Einhaltung der geltenden Gesetzgebung durch die Verwaltungs- und Kontrollorgane, Mitarbeiter, Mitarbeiter und Berater des Unternehmens sicherzustellen. Diese Kontrollen stehen auch im Einklang mit den im Datenschutzgesetz festgelegten Regeln und Verfahren.

Das Unternehmen verlässt sich auch auf Indikatoren für Anomalien und Muster unregelmäßigen Verhaltens im Wirtschafts- und Finanzumfeld, die im Laufe der Zeit von der Financial Intelligence Unit (FIU) im Hinblick auf potenzielle Geldwäsche- und Terrorismusfinanzierungsaktivitäten herausgegeben werden.

2.2 - DER REGELUNGSRAHMEN FÜR RESTRIKTIVE MASSNAHMEN UND EMBARGOS

Alle restriktiven Maßnahmen zur Bekämpfung der Finanzierung des Terrorismus und aller illegalen oder verdächtigen Aktivitäten, die den Weltfrieden und die internationale Sicherheit gefährden, können entweder kommerzieller Natur sein, etwa Import-/Exportbeschränkungen aus/in ein Land, oder finanzieller Natur, etwa die teilweise oder vollständige Blockierung des Geldtransfers, aber auch operative Beschränkungen und das Einfrieren von Geldern.

Zu den restriktiven Maßnahmen gehören internationale Finanzsanktionen, auch Embargos genannt, die vom italienischen Staat, ausländischen Behörden (z. B. OFAC, UKSL) und supranationalen Organisationen (UN, EU) durch eine Reihe von Verpflichtungen umgesetzt werden, die das Unternehmen einhalten muss. Zur Umsetzung der vom UN-Sicherheitsrat gemäß Kapitel VII der UN-Charta angenommenen Resolutionen werden vom Rat bestimmte restriktive Maßnahmen (Sanktionen) gegen alle UN-Mitgliedstaaten verhängt. Darüber hinaus können Sanktionen von der Europäischen Union durch Verordnungen des Rates verabschiedet oder autonom beschlossen werden, die in jedem Mitgliedstaat sofort durchsetzbar sind, um ihre rechtzeitige und gleichzeitige Anwendung sicherzustellen.

Auf internationaler Ebene gibt es Vorschriften, die spezifische Verbote oder Beschränkungen für Investitionen in bestimmte Industriesektoren oder den Import/Export aus/in „Länder mit hohem oder erheblichem Risiko" festlegen. Dabei geht es insbesondere um Resolutionen des UN-Sicherheitsrates (UNSC) gemäß Artikel 41 des Kapitels VII der UN-Charta, durch die restriktive Maßnahmen gegenüber Personen und/oder Ländern verhängt werden.

Die wichtigsten Bestimmungen des Gemeinschaftsrechts sind:

- die Verordnung 2021/821 des Europäischen Parlaments und des Rates vom 20. Mai 2021[3] **und nachfolgende Änderungen, durch die ein EU-Regime zur Kontrolle von Exporten, Transfer, Vermittlung und Transit von Gütern mit doppeltem Verwendungszweck eingeführt wird;**

3, die die Verordnung 428/2009/EG des Rates vom 5. Mai 2009 ersetzte

- die Verordnung (EU) 2023/1113 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über Informationen bei Geldtransfers und bestimmten Kryptowerten und zur Änderung der Richtlinie (EU) 2015/849 (Neufassung);
- die Verordnung (EU) 2024/886 des Europäischen Parlaments und des Rates vom 13. März 2024 zur Änderung der Verordnungen (EU) Nr. 260/2012 und (EU) 2021/1230 sowie der Richtlinien 98/26/EG und (EU) 2015/2366 in Bezug auf Sofortüberweisungen in Euro;
- die Richtlinie (EU) 2024/1226 des Europäischen Parlaments und des Rates vom 24. April 2024 über die Definition von Straftaten und Strafen für Verstöße gegen restriktive Maßnahmen der Union und zur Änderung der Richtlinie (EU) 2018/1673, umgesetzt in italienisches Recht durch das Gesetzesdekret 211/2025.
- **Leitlinien der Europäischen Bankenaufsichtsbehörde zu internen Richtlinien, Verfahren und Kontrollen zur Gewährleistung der Umsetzung restriktiver Maßnahmen der Union und der Mitgliedstaaten (EBA/GL/2024/14)**[4];
- **Leitlinien der Europäischen Bankenaufsichtsbehörde zu internen Richtlinien, Verfahren und Kontrollen zur Gewährleistung der Umsetzung restriktiver Maßnahmen der Union und der Mitgliedstaaten gemäß der Verordnung (EU) 2023/1113 (EBA/GL/2024/15) über Informationen bei Geldtransfers und bestimmten Kryptowerten und zur Änderung der Richtlinie (EU) 2015/849**[5].

Auf nationaler Ebene werden Embargos schließlich wie folgt geregelt:

- **Primäre Gesetzgebung:**
  - **Gesetzesdekret Nr. 221/2017, mit dem die Genehmigungsverfahren für den Export von Gütern und Technologien mit doppeltem Verwendungszweck sowie Sanktionen für Handelsembargos sowie alle Arten von Exportvorgängen für sich vermehrende Materialien geändert und vereinfacht wurden.**
- **Sekundärgesetzgebung:**
  - **Bestimmung der Bank von Italien vom 12. Mai 2023 mit Anomalieindikatoren für Vermittler, um die Identifizierung verdächtiger Transaktionen zu erleichtern.**

Schließlich sind alle von den US-Behörden erlassenen Vorschriften für die Tätigkeit des Unternehmens im Hinblick auf Reputationsaspekte und den Verweis auf diese Vorschriften bei vertraglichen Vereinbarungen, die die mögliche Anwendung von Sanktionen mit extraterritorialer Wirkung (sog. „Sekundärsanktionen" der USA) beinhalten, relevant. Solche Regulierungsbestimmungen sind im USA Patriot Act6 und in den Maßnahmen zu Wirtschafts- und Handelssanktionen enthalten, die von der US-Regierung über das Office of Foreign Assets Control (OFAC) des Finanzministeriums erlassen wurden.[6]

4, deren Einhaltung die Bank von Italien in Anmerkung Nr. 48 vom 8. April 2025 und gültig ab 30. Dezember 2025.

5, deren Einhaltung die Bank von Italien in Anmerkung Nr. 52 vom 19. Mai 2025 und gültig ab 30. Dezember 2025.

6 US-Bundesgesetz vom 26. Oktober 2001 mit dem offiziellen Titel „Amerika vereinen und stärken durch die Bereitstellung geeigneter Werkzeuge, die zum Abfangen und Verhindern des Terrorismus erforderlich sind" (Gesetz von 2001).

3 – GRUPPENMODELLE UND METHODEN

3.1 – ALLGEMEINE ASPEKTE

Der etablierte nationale Regulierungsrahmen für präventive Maßnahmen gegen Geldwäsche, Terrorismusfinanzierung und Verstöße gegen die restriktiven Maßnahmen basiert auf einer Reihe von Verpflichtungen

dass die Empfänger Folgendes respektieren müssen:

- Verpflichtung zur Einführung geeigneter Organisationsstrukturen, Verfahren und interner Kontrollmaßnahmen;
- Verpflichtung, konsistente und kohärente Verfahren zur Analyse und Bewertung der Risiken im Zusammenhang mit Geldwäsche, Terrorismusfinanzierung und Verstößen gegen die restriktiven Maßnahmen einzuführen sowie Aufsicht, Kontrollen und Verfahren einzurichten, die zur Minderung und Bewältigung dieser Risiken erforderlich sind;
- Verpflichtung zur Sorgfaltspflicht gegenüber dem Kunden, durch die das Unternehmen Informationen über die Identität eines Kunden und etwaiger wirtschaftlicher Eigentümer sowie den Zweck und die beabsichtigte Art der Beziehung oder der Transaktion erwirbt und überprüft und gleichzeitig die ständige Überwachung aller vom Kunden durchgeführten Transaktionen gewährleistet;
- ein risikobasierter Ansatz, bei dem die Sorgfaltspflichten des Kunden entsprechend dem Risikoprofil des Kunden in verschiedene Sorgfaltsgrade unterteilt werden;
- Verpflichtung zur Aufbewahrung von Dokumenten, Daten und Informationen, um deren rechtzeitige Erfassung, Transparenz, Vollständigkeit, Unveränderlichkeit und Integrität sowie eine umfassende und zeitnahe Zugänglichkeit zu ermöglichen;
- Verpflichtung zur Meldung verdächtiger Transaktionen;
- Verpflichtung, keine neue Kundenbeziehung einzugehen, gelegentliche Transaktionen durchzuführen oder eine bestehende Kundenbeziehung aufrechtzuerhalten, wenn keine Sorgfaltspflichten eingehalten wurden oder der Verdacht besteht, dass ein Zusammenhang mit Geldwäsche oder Terrorismusfinanzierung bestehen könnte;
- Verpflichtung, das Ministerium für Wirtschaft und Finanzen über die in den Artikeln 49 und 50 des Gesetzesdekrets 231/07 genannten Verstöße zu informieren und die Beschränkungen für die Verwendung von Bargeld und Inhaberpapieren einzuhalten;
- Überwachung aller Transaktionen mit natürlichen und juristischen Personen und/oder mit Ländern, die in den Listen des Rates der Europäischen Union (UE), in der Office of Foreign Assets Control List (OFAC) und in der UK Sanctions List (UKSL) aufgeführt sind.[7], in der Konsolidierten Sanktionsliste des Sicherheitsrats der Vereinten Nationen (UN) in den von den nationalen Behörden erlassenen Bestimmungen, die spezifische restriktive Maßnahmen zur Terrorismusbekämpfung enthalten;
- Überwachung von Transaktionen mit Ländern, die in Steuer-, Finanzaufsichts- und Geldwäschebekämpfungsfragen als nicht kooperativ gelten und im Allgemeinen als „Steueroasen" oder „Offshore-Finanzzentren" bezeichnet werden;
- Einführung geeigneter Schulungsprogramme für das Personal, um die Umsetzung und ordnungsgemäße Anwendung von Gesetzen und Vorschriften sicherzustellen;
- Verpflichtung, der FIU „objektive Mitteilungen" gemäß den spezifischen Bestimmungen bereitzustellen
  Anweisungen zu Methoden und Häufigkeit der Kommunikation;

7 Die OFSI-Liste (Office of Financial Sanctions Implementation HMT) wurde am 28. Januar 2026 geschlossen; Ab diesem Datum ist die UK Sancti ons List die einzige offizielle Quelle für alle Sanktionen im Vereinigten Königreich.

- Verpflichtung zur Offenlegung aller Verstöße oder Verstöße, die den Kontrollstellen bei der Wahrnehmung ihrer Aufgaben zur Kenntnis gelangen könnten;
- Verpflichtung zur Einführung von Verfahren zur Verwaltung der internen Meldung von Verstößen durch Mitarbeiter (Whistleblowing).

Im Hinblick auf Aktivitäten zur Bekämpfung der Terrorismusfinanzierung verlangt die italienische Gesetzgebung von den verpflichteten Parteien Folgendes:

- Einfrieren von Geldern und wirtschaftlichen Ressourcen bestimmter Personen, die in EU-Listen aufgeführt sind;
- Benachrichtigung der Financial Intelligence Unit (FIU) über die Maßnahmen, die zum Einfrieren von Geldern ergriffen wurden, oder der Sonderwährungspolizeieinheit der Guardia di Finanza (Finanzpolizei) im Falle wirtschaftlicher Ressourcen;
- Benachrichtigung der FIU über verdächtige Transaktionen, Geschäftsbeziehungen und alle anderen verfügbaren Informationen über Parteien, die in den von der FIU selbst veröffentlichten schwarzen Listen aufgeführt sind;
- Meldung verdächtiger Transaktionen, die auf der Grundlage der verfügbaren Informationen direkt oder indirekt mit Aktivitäten zur Terrorismusfinanzierung in Zusammenhang stehen.

Im Hinblick auf internationale Sanktionen (sogenannte Embargos) und die Gefährdung durch restriktive Maßnahmen schreibt die Gesetzgebung die Ergreifung bestimmter Maßnahmen vor, darunter unter anderem:

- Personenbezogene Daten und Transaktionskontrollen bei Vorgängen im Zusammenhang mit Importen und/oder Exporten, die von Kunden durchgeführt werden, mit dem Ziel, Importe/Exporte aus oder in ein Land zu blockieren, sowie entsprechende Vorschriften. Das Verbot kann entweder allgemein sein und alle Arten von Waren umfassen, sofern nicht ausdrücklich genehmigt, oder auf bestimmte Arten von Waren beschränkt sein, z. B. Rüstungsgüter (siehe Zollkodex);
- vollständige oder teilweise Beschränkungen für Finanztransfers von/in ein Land;
- vorherige Genehmigungspflicht zur Durchführung von Überweisungen;
- Meldepflicht für Übertragungen (ausgehend oder eingehend);
- Verbot der Finanzierung, Bereitstellung von Finanzhilfen oder der Bereitstellung subventionierter Kredite für die Regierung (direkt oder in einigen Fällen indirekt über verbundene Unternehmen oder die Beteiligung an internationalen Finanzinstitutionen);
- Verbot der Finanzierung von Kunden, die mit sanktionierten Ländern operieren;
- Umsetzung restriktiver Maßnahmen gegen russische und weißrussische Untertanen;
- die Rückverfolgbarkeit von Kontrollen, die bei Vorgängen durchgeführt werden, die aus Ländern, Personen und Organisationen stammen oder an diese gerichtet sind und Beschränkungen unterliegen.

3.2 - DUE DILIGENCE DES KUNDEN

3.2.1 – Allgemeine Aspekte

Das Unternehmen ergreift alle Due-Diligence-Maßnahmen gegenüber Kunden, wenn:

- Aufbau von Geschäftsbeziehungen;

- Durchführung gelegentlicher, von Kunden arrangierter Transaktionen, wie z. B. Banküberweisungen oder andere Transaktionen, die den geltenden festgelegten Schwellenwert erreichen oder überschreiten, unabhängig davon, ob die Transaktion in einem einzigen Vorgang oder in mehreren verbundenen Vorgängen durchgeführt wird oder ob es sich um einen Geldtransfer handelt, der die gesetzlichen Grenzen überschreitet;

- Es besteht der Verdacht auf Geldwäsche oder Terrorismusfinanzierung, ungeachtet etwaiger Ausnahmeregelungen, Befreiungen oder festgelegter Schwellenwerte;
- Es bestehen Zweifel an der Vollständigkeit, Zuverlässigkeit und Richtigkeit der zuvor zur Identifizierung eines Kunden eingeholten Informationen oder Unterlagen.

Sorgfaltspflichten:

- sind erfüllt:
  - gegenüber Neukunden vor dem Aufbau einer laufenden Beziehung oder der Durchführung einer gelegentlichen Transaktion;
  - gegenüber bestehenden Kunden, wenn angesichts einer Änderung des Ausmaßes des Geldwäsche- oder Terrorismusfinanzierungsrisikos, das mit dem Kunden verbunden ist, oder wenn Verdachtsmomente oder Zweifel an der Richtigkeit oder Angemessenheit der zuvor vom Kunden erhaltenen Informationen bestehen, eine angemessene Sorgfaltspflicht geboten ist;

- und bestehen aus folgenden Aktivitäten:
  - Identifizierung des Kunden, des wirtschaftlichen Eigentümers und des Testamentsvollstreckers und Überprüfung ihrer Identität anhand von Dokumenten, Daten oder Informationen, die von einer zuverlässigen und unabhängigen Quelle stammen;
  - Einholung und Beurteilung von Informationen über den Zweck und die beabsichtigte Art der Geschäftsbeziehung;
  - Durchführen einer kontinuierlichen Überwachung während der gesamten Dauer der Kundenbeziehung.

Zu diesem Zweck holt das Unternehmen über seine Mitarbeiter und/oder über Agenten/Finanzberater, die berechtigt sind, Angebote außerhalb der Geschäftsräume abzugeben und in direkten Kontakt mit dem Kunden treten, die gemäß den Vorschriften erforderlichen Informationen ein und sammelt alle anderen relevanten Unterlagen gemäß dieser Richtlinie und den Verfahrensunterlagen des Unternehmens.

Das Unternehmen wendet gewöhnliche, vereinfachte oder erweiterte Kunden-Due-Diligence-Maßnahmen entsprechend dem risikobasierten Ansatz für Kunden an.

3.2.2 - Kunden-Remote-Onboarding

In Fällen, in denen das Unternehmen Fernidentifizierungsmethoden verwendet, wie durch das Gesetzesdekret Nr. 231/07, Art. 19 Abs. 1 Buchst. a Ziff. 2 und 5, legt es besondere Verfahren zur Erfüllung seiner Sorgfaltspflichten fest, auch im Hinblick auf das mit Identitätsdiebstahl verbundene Betrugsrisiko. In diesem Fall basiert die Identifizierung auf dem Erwerb des qualifizierten elektronischen Signaturzertifikats, das nach einem Identifizierungsprozess generiert wird, der durchgeführt wird durch:

- die Verwendung des öffentlichen digitalen Identitätssystems (SPID) oder des elektronischen Personalausweises;
- mittels sicherer und regulierter elektronischer Identifizierungstechniken und -verfahren, die von der Agentur für Digitales Italien autorisiert oder anerkannt sind.

In allen Fällen umfasst der Fernidentifizierungsprozess die Erfassung der Identifikationsdaten

des Kunden und eines etwaigen Testamentsvollstreckers in elektronischer Form sowie die Durchführung von Überprüfungen und Überprüfungen der Authentizität der Daten, zusätzlich zu denen, die für die persönliche Identifizierung vorgesehen sind, nach einem risikobasierten Ansatz, unter anderem durch Telefonkontakt unter einer zertifizierten Nummer (Begrüßungsanruf) oder eine vom Kunden über einen in Italien ansässigen Bank- und Finanzintermediär durchgeführten Geldüberweisung.

Um die Gefährdung durch potenzielle Geldwäsche- und/oder Betrugsrisiken zu begrenzen, ist der Aufbau von Remote-Banking-Beziehungen mit juristischen Personen oder natürlichen Personen, die im Namen einer juristischen Person handeln, nicht gestattet, es sei denn, diese wurden persönlich (persönlich) identifiziert.

Der Aufbau von Remote-Banking-Beziehungen mit Kunden, die nicht in Italien ansässig sind, ist nicht gestattet.

3.2.3 – Bewertung vor der Implementierung und laufende Überwachung der Prozesse zur Eröffnung von Remote-Beziehungen.

Die Prozesse der Remote-Kundenidentifizierung und des Onboardings sind in den internen Vorschriften formalisiert und detailliert. Das Modell zur Überwachung dieser Prozesse umfasst:

I. die vorläufige Bewertung der Remote-Onboarding-Lösung (sog. Pre-Implementation Assessment).[8]) richtet sich an:
   (i) Beurteilung der Angemessenheit der Lösung im Hinblick auf die Vollständigkeit und Richtigkeit der zu erhebenden Daten und Dokumente sowie die Zuverlässigkeit und Unabhängigkeit der verwendeten Informationsquellen;
   (ii) Bewerten Sie die Auswirkungen des Einsatzes der Lösung auf Geschäftsrisiken, einschließlich Betriebs-, Reputations- und Rechtsrisiken, durch Einbeziehung der relevanten technischen und spezialisierten Funktionen.
   (iii) Ermittlung von Abhilfemaßnahmen und Korrekturmaßnahmen für jedes identifizierte Risiko;
   (iv) Definieren Sie Ex-ante-Tests zur Bewertung von IKT- und Betrugsrisiken sowie End-to-and-Tests für den Betrieb der Lösung.

II. Laufende Überwachung der eingeführten Onboarding-Lösung durch regelmäßige und ereignisgesteuerte Kontrollen, um sicherzustellen, dass sie im Laufe der Zeit ordnungsgemäß funktioniert (sog. laufende Überwachung).

III. die Überprüfung der vorläufigen Bewertung in der Remote-Onboarding-Lösung (sog. Pre-Implementation Assessment), wenn strukturelle Änderungen in der übernommenen Lösung oder bestimmte Ereignisse eintreten, wie zum Beispiel:
   (i) Veränderungen der Risikoexposition in den Bereichen Geldwäschebekämpfung und Bekämpfung der Terrorismusfinanzierung sowie Embargos;
   ii) erkannte Mängel, damit unsere Lösung funktioniert;
   iii) eine Zunahme von Betrugsversuchen;
   (iv) Gesetzesänderungen.

3.2.4 – Vereinfachte Sorgfaltspflichten

Im Allgemeinen verwendet das Unternehmen einen risikobasierten Ansatz, um die Arten von Kunden zu identifizieren, auf die vereinfachte Due-Diligence-Maßnahmen angewendet werden können. Dazu gehören Fälle, in denen „Indikatoren für ein geringes Risiko" vorliegen, wie in Anhang 1 der Bestimmung der Bank von Italien über die Sorgfaltspflicht gegenüber Kunden vom 30. Juli 2019 (im Folgenden „die Bestimmung") angegeben.

8 Note Nr. 32 vom 13. Juni 2023, mit der die Bank von Italien ihre Absicht bekundete, die EBA-Leitlinien (EBA/GL/2022/15) zum Einsatz von Remote-Onboarding-Lösungen für Kunden einzuhalten.

Die für die Anwendung eines vereinfachten Due-Diligence-Verfahrens relevanten „Indikatoren für geringes Risiko" basieren auf der Art des Kunden, Ausführenden oder wirtschaftlichen Eigentümers, dem geografischen Gebiet, in dem sich der Wohnsitz befindet oder in dem sich der Hauptsitz befindet, sowie auf dem spezifischen Produkt, der Dienstleistung oder dem Vertriebskanal.

Zu den Kundentypen mit geringem Geldwäscherisiko, für die die vereinfachte Sorgfaltspflicht gelten kann, gehören im Einzelnen:

- Öffentliche Verwaltungen, Institutionen oder Einrichtungen, die gemäß dem Recht der Europäischen Union öffentliche Aufgaben wahrnehmen;
- Unternehmen, die an einem geregelten Markt notiert sind und Offenlegungspflichten unterliegen, einschließlich der Gewährleistung einer angemessenen Transparenz des letztendlichen wirtschaftlichen Eigentums;
- die Kredit- und Finanzinstitute der Europäischen Gemeinschaft, die in Artikel 3 Absatz 2 der Verordnung zur Bekämpfung der Geldwäsche aufgeführt sind – mit Ausnahme derjenigen, die unter den Buchstaben i), o), s), v) aufgeführt sind[9]— und die Kredit- und Finanzinstitute mit Sitz in Mitgliedstaaten oder Drittländern mit wirksamen Geldwäsche- und Terrorismusfinanzierungssystemen;
- Kunden, Testamentsvollstrecker oder wirtschaftliche Eigentümer, die in geografischen Gebieten mit geringem Geldwäscherisiko ansässig oder niedergelassen sind.

Das Unternehmen wendet keine vereinfachten Kunden-Due-Diligence-Maßnahmen an, wenn:

- Zweifel, Unsicherheiten oder Inkonsistenzen hinsichtlich der identifizierenden Daten und Informationen entstehen, die bei der Identifizierung des Kunden, Testamentsvollstreckers oder wirtschaftlichen Eigentümers gesammelt wurden;
- die Voraussetzungen für eine vereinfachte Kundensorgfalt sind aufgrund der in der Geldwäschereiverordnung und der einschlägigen Sekundärverordnung vorgesehenen Risikoindikatoren nicht mehr gegeben;
- Die Überwachung der gesamten vom Kunden durchgeführten Vorgänge und die während der Geschäftsbeziehung gesammelten Informationen schließen einen Typ mit geringem Risiko aus;
- weiterhin der Verdacht der Geldwäsche oder Terrorismusfinanzierung besteht.

Die Anti-Geldwäsche-Funktion trägt die ausschließliche Verantwortung für die Bewertung und Genehmigung vereinfachter Kunden-Due-Diligence-Maßnahmen. Dabei werden alle Schritte befolgt, die für den normalen Kunden-Due-Diligence-Prozess erforderlich sind – einschließlich der Verpflichtung, die Identität des Kunden, des Testamentsvollstreckers und des wirtschaftlichen Eigentümers zu identifizieren und zu überprüfen und alle für ihre vollständige Registrierung erforderlichen Daten und Dokumente zu beschaffen (z. B. Name, Rechtsstatus, eingetragener Sitz und gegebenenfalls Steuernummer), allerdings mit einer Reduzierung ihrer Tiefe, ihres Umfangs und ihrer Häufigkeit.

3.2.5 – Erweiterte Sorgfaltspflichten

Das Unternehmen wendet bei Kunden oder in Situationen mit einem höheren Risiko der Geldwäsche oder Terrorismusfinanzierung sowie in allen in Artikel 24 des Erlasses genannten Fällen verstärkte Sorgfaltspflichten gegenüber Kunden an. Zu diesen erweiterten Maßnahmen gehört unter anderem die Einbeziehung verantwortlicher Rollen, die dem in Bezug auf den Kunden festgestellten Risikoniveau angemessen sind.

9 i) Börsenmakler im Sinne von Artikel 201 TUF; o) Versicherungsvermittler gemäß Artikel 109 Absatz 2 Buchstaben a), b) und d) der GAP, die in den in Artikel 2 Absatz 1 der GAP genannten Tätigkeitsbereichen tätig sind; s) Treuhandgesellschaften, die im gemäß Artikel 106 TUB eingerichteten Register eingetragen sind; v) Finanzberater gemäß Artikel 18-bis des TUF und Finanzberatungsunternehmen gemäß Artikel 18-ter des TUF.

Bei Private-Banking-Kunden bewertet das Unternehmen die spezifischen Risikofaktoren, die mit der Art ihres Geschäfts einhergehen, und wendet auf der Grundlage der verfügbaren Gesamtinformationen und der durchgeführten Bewertungen verstärkte Sorgfaltsmaßnahmen an.

Die Einschaltung der Geldwäschebekämpfungsstelle ist in folgenden Fällen erforderlich:

- natürliche und juristische Personen, die in den Listen der Personen oder Organisationen aufgeführt sind, die aufgrund europäischer Verordnungen oder Dekrete gemäß Gesetzesdekret 109/07 Maßnahmen zum Einfrieren von Geldern unterliegen, sowie diejenigen, die eng mit ihnen verbunden sind;
- eine grenzüberschreitende Korrespondenzbankbeziehung mit einer Bank oder einem Institut mit Sitz in einem Drittland, basierend auf geografischen Hochrisikofaktoren (wie in Anhang 2 der Bestimmungen der Bank von Italien zur Sorgfaltspflicht gegenüber Kunden aufgeführt);
- Beziehungen oder Transaktionen, bei denen der Kunde oder letztendliche wirtschaftliche Eigentümer eine politisch exponierte Person ist[10];
- Situationen mit Risikoelementen, die die Anwendung spezifischer Vertraulichkeitsmaßnahmen erfordern;
- Situation mit einem höheren Risiko der Geldwäsche oder Terrorismusfinanzierung aufgrund objektiver, umweltbedingter oder subjektiver Eventualitäten;
- Kunden, die als „Trust", Geldtransferdienste und virtuelle Währungsumtausche klassifiziert sind;
- Vertrauensunternehmen, außer wie in Absatz 3.4 vorgesehen;

Darüber hinaus ist es vor dem Eingehen, Fortführen oder Aufrechterhalten einer laufenden Beziehung mit politisch exponierten Personen oder korrespondierenden Unternehmen aus Drittländern erforderlich, die entsprechende Genehmigung des Geschäftsführers oder seines Beauftragten einzuholen, nachdem die Stellungnahme der Anti-Geldwäsche-Funktion eingeholt wurde. Im Falle von Beauftragten gemäß Artikel 25 des Gesetzesdekrets 231/07, die der Funktion zur Bekämpfung der Geldwäsche angehören, ist diese Ermächtigung in den Prozess der verstärkten Sorgfaltspflicht einbezogen.

In allen anderen Fällen steht die Anwendung erweiterter Maßnahmen in einem angemessenen Verhältnis zum Grad des dem Kunden zugeschriebenen Risikos. Wird das Risiko als mittel/hoch eingestuft oder liegen unabhängig von der vergebenen Bewertung bestimmte Risikofaktoren vor, ist die Einbindung des für die kaufmännische Betreuung des Kunden verantwortlichen Leiters der Geschäftseinheit erforderlich.

Beispiele für solche Fälle sind:

- Kunden juristischer Personen mit einem Testamentsvollstrecker, der unabhängig vom Risikoprofil als PEP oder indirekter PEP identifiziert wurde;
- Dienstleistungen, die über Netzwerke von Finanzagenten, Finanzberatern, Auftragnehmern und Agenten angeboten werden;
- Kunden, die als Stiftungen/gemeinnützige Organisationen klassifiziert sind;
- Kunden juristischer Personen während der Onboarding-Phase;
- Kunden mit negativen Nachrichten während der Onboarding-Phase („Adverse News");

10 Politisch exponierte Personen (PEPs): gemäß Art. 1, Absatz 2, Buchstabe dd) Gesetzesdekret 231/07.

- Kunden mit Wohnsitz oder Sitz in Drittländern mit hohem Risiko oder im Falle laufender Beziehungen, professioneller Dienstleistungen und Geschäftstätigkeiten, an denen Länder mit hohem Risiko beteiligt sind;
- Unternehmen, die Inhaberaktien ausgegeben haben oder in deren Kontrollkettenstruktur sich ein Unternehmen befindet, das Inhaberaktien ausgibt;
- Beziehungen oder Transaktionen, bei denen der Kunde und der letztendliche wirtschaftliche Eigentümer ein anderes öffentliches Amt innehaben als die für politisch exponierte Personen aufgeführten[11];
- Unternehmen im Besitz von Trusts, Treuhandgesellschaften, Stiftungen, Aktiengesellschaften über mehrere Beteiligungsebenen oder Kreuzbeteiligungen;
- Kunden, die einer Wirtschaftstätigkeit nachgehen, die besonders dem Risiko der Geldwäsche ausgesetzt ist, oder in „umstrittenen" Tätigkeitsbereichen tätig sind[12] oder bargeldintensive kommerzielle Aktivitäten wie Bargeld gegen Gold, Geldwechsel, Glücksspiele/Wetten, auch online, Rüstungsindustrie, Bergbau, Abfallsammlung und -entsorgung, Produktion erneuerbarer Energien, Unternehmen, die im Krypto-Asset-Sektor tätig sind, Bauwesen, Beschaffung von pharmazeutischen Instrumenten;
- Kunden, die an öffentlichen Aufträgen teilnehmen oder öffentliche Mittel erhalten (Gesundheitswesen, Bauwesen, Abfallsammlung und -entsorgung, Produktion erneuerbarer Energien, Bergbau, Lieferung pharmazeutischer Instrumente);
- im Falle von Kunden, die die Staatsbürgerschaft eines Mitgliedstaats erworben haben oder Aufenthaltsrechte in einem Mitgliedstaat (EU) durch ein Staatsbürgerschafts-durch-Investitionsprogramm oder ein Aufenthaltsrecht durch Investition-Programm erlangt haben;
- bei juristischen Personen des Kunden mit Sitz in einem EU-Land, bei denen die Eigentumsrechte des Unternehmens – direkt oder indirekt – zu mehr als 40 % von einer in Russland ansässigen juristischen Person, Organisation oder Einrichtung oder einer natürlichen Person mit russischem Wohnsitz oder russischer Staatsbürgerschaft gehalten werden.

Auch bei IT-Fehlern, die eine Echtzeitberechnung des Geldwäscherisikos des Kunden verhindern könnten, ist die Einbindung des für die kaufmännische Betreuung des Kunden verantwortlichen Bereichsleiters erforderlich.

Zu den verstärkten Due-Diligence-Maßnahmen gehören die Beschaffung zusätzlicher Informationen über den Kunden, den Testamentsvollstrecker und den wirtschaftlichen Eigentümer, die Untersuchung des Zwecks und der Art der Beziehung sowie die Erhöhung der Häufigkeit von Verfahren, um eine kontinuierliche Überwachung während der laufenden Beziehung sicherzustellen.

In voller Übereinstimmung mit der geltenden Gesetzgebung und den Bestimmungen der internen Verfahren zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung sowie im Einklang mit dem Ethikkodex des Unternehmens unterstützt das Unternehmen keine Transaktionen mit Kunden, die in umstrittenen Sektoren tätig sind
(i) den geltenden nationalen Rechtsvorschriften nicht entsprechen und (ii) gegebenenfalls nicht im Voraus von den zuständigen italienischen Behörden genehmigt wurden, insbesondere:

- die Produktion, der Transport und/oder die Vermarktung von Rüstungsgütern;
- die Produktion und der Verkauf von leichtem Marihuana, Veranstaltungsorte für Erwachsenenunterhaltung;

11 Öffentliche Ämter, die nicht von politisch exponierten Personen (PEPs) gemäß Anmerkung 1 bekleidet werden, gelten für alle Personen, die ein Amt in öffentlichen Einrichtungen, Konsortien und Vereinigungen öffentlicher Natur innehaben, wie in Abschnitt A 8) von Anhang 2 der Bestimmung aufgeführt.
12 Ein Wirtschaftszweig ist „umstritten", wenn die hergestellten/angebotenen Güter/Dienstleistungen und/oder die Art und Weise, wie sie produziert/angeboten werden, im Widerspruch zu den weit verbreiteten Werten der Ethik und Nachhaltigkeit stehen, auch wenn Dienstleistungen oder Tätigkeiten rechtmäßig sind und daher nicht im Widerspruch zu rechtlichen Verpflichtungen stehen.

- Andere als die oben aufgeführten bargeldintensiven kommerziellen Aktivitäten, wie z. B. nicht regulierte Wohltätigkeitsorganisationen und NGOs, die Produktion von Edelmetallen und Steinen, Geldüberweisungen.

Darüber hinaus achtet das Unternehmen besonders auf die Einhaltung restriktiver Maßnahmen des italienischen Staates, ausländischer Stellen (z. B. OFAC, UKSL) und/oder supranationaler Stellen (UN, EU). Diese Maßnahmen können kommerzieller Natur (z. B. Blockierung von Importen/Exporten) oder finanzieller Natur sein, wie z. B. eine teilweise oder vollständige Blockierung von Geldtransfers von oder in ein bestimmtes Land oder Beschränkungen des Geschäftsbetriebs und/oder das Einfrieren von Geldern bei Finanzintermediären.

Zur Einhaltung der im italienischen Gesetzesdekret 109/07 festgelegten Verpflichtungen – die darauf abzielen, die Finanzierung des Terrorismus und die Aktivitäten von Ländern, die den Weltfrieden und die internationale Sicherheit gefährden, zu verhindern und zu bekämpfen, und zwar durch die Anwendung restriktiver Maßnahmen zum „Einfrieren" von Geldern und wirtschaftlichen Ressourcen, die von natürlichen und juristischen Personen, Gruppen und Körperschaften gehalten werden, die von den Vereinten Nationen und der Europäischen Union ausdrücklich identifiziert wurden („designierte Subjekte") – und den im italienischen Gesetzesdekret festgelegten erweiterten Sorgfaltspflichten 231/07 hat das Unternehmen automatische Kontrollverfahren eingeführt. Diese Verfahren sind in der Lage, die Konsistenz zwischen den im Rahmen des Due-Diligence-Prozesses erhaltenen Kundenidentifikationsdaten und den in den von der EU und anderen internationalen Institutionen und Gremien erstellten Listen enthaltenen Daten zu überprüfen, wie zum Beispiel:

- Personen, die mit einem wichtigen öffentlichen Amt betraut sind oder dieses Amt seit weniger als einem Jahr nicht mehr ausüben (PEP), deren Familienangehörige und mit ihnen in enger Beziehung stehende Personen im Sinne des Art. 1 c. 2 Buchstabe dd des Gesetzesdekrets 231/07 (gebietsansässige und gebietsfremde PEPs);
- Personen mit Wohnsitz in Italien, die ein öffentliches Amt bekleiden, die nicht unter die Definition von PEPs fallen, aber dennoch einem erheblichen Risiko von Korruption und Geldwäsche ausgesetzt sind;
- natürliche und juristische Personen, die, auch teilweise, in Staaten tätig sind, die keine gleichwertigen Maßnahmen und Vorschriften gemäß den Richtlinien der Bank von Italien oder anderen nationalen oder supranationalen Institutionen, die sich mit der Kriminalitätsverhütung befassen, vorschreiben;
- natürliche und juristische Personen, die Embargomaßnahmen oder dem Einfrieren von Geldern/wirtschaftlichen Ressourcen und finanziellen Vermögenswerten unterliegen (Sanktionslisten UN, EU, UKSL, OFAC).

3.3 - KUNDENPROFILIERUNG

Das Unternehmen wendet geeignete Verfahren an, die darauf abzielen, das jedem Kunden zuzuordnende Geldwäsche- und Terrorismusfinanzierungs-Risikoprofil (RPs) auf der Grundlage der erfassten Informationen und durchgeführten Analysen zu definieren, und zwar sowohl unter Bezugnahme auf die in der Bestimmung genannten Bewertungselemente als auch auf weitere Elemente, die das Unternehmen im Laufe der Zeit selbst übernehmen kann (sogenanntes Profiling).

Auf der Grundlage der Kundenprofilierung, die ebenfalls regelmäßig durchgeführt wird, wendet

das Unternehmen Standard- oder erweiterte Maßnahmen an, zu denen auch die Einbindung von Verantwortlichen gehört, die dem identifizierten Risikoniveau des Kunden entsprechen. Gemäß den im internen Dokument „Interne Verfahren zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung" festgelegten Zuständigkeiten ist die vorherige Stellungnahme der Anti-Geldwäsche-Funktion erforderlich.

Die Einstufung von Kunden für vereinfachte Sorgfaltspflichten wird von der Anti-Geldwäsche-Funktion auf Antrag des Leiters der operativen Geschäftseinheit genehmigt.

In einem solchen Fall werden Umfang und Häufigkeit der Anforderungen reduziert, wobei die Überprüfung unabhängig von der Risikobewertung nach 8 Jahren endet, es sei denn, die Voraussetzungen für die Anwendung vereinfachter Sorgfaltspflichten sind nicht mehr gegeben.

Darüber hinaus hat das Unternehmen ein IT-Verfahren eingeführt, um das Risikoprofil des Kunden zu bewerten und konsequent einen Zeitrahmen für die Neubewertung festzulegen, der dem berechneten Risikoniveau entspricht. Die Häufigkeit der Neubewertung hängt von dem bei der letzten durchgeführten Bewertung identifizierten Prozess ab oder, falls kein KYC-Fragebogen vorliegt, vom Risikoprofil des Kunden, wie unten angegeben:

<table>
<tr><th>Risikoklasse (RP)</th><th>Punktzahl</th><th>Due-Diligence-Prozess</th><th>Validierungsrolle</th><th>Häufigkeit der Neubewertung</th></tr>
<tr><td>Kunden, die der vereinfachten Sorgfaltspflicht unterliegen</td><td>NA</td><td>Vereinfacht</td><td>Automatische Annahme/Business Unit Manager (*)</td><td>8 Jahre</td></tr>
<tr><td>Immateriell</td><td><=5</td><td rowspan="2">Standard</td><td rowspan="2">Automatische Annahme</td><td>8 Jahre</td></tr>
<tr><td>Niedrig</td><td>>=6 e <=12</td><td>6 Jahre</td></tr>
<tr><td>Mittel</td><td>>=13 e <=24</td><td rowspan="2">Verbessert</td><td rowspan="2">Geschäftsbereichsleiter (**)</td><td>2 Jahre</td></tr>
<tr><td>Hoch</td><td>>=25</td><td>1 Jahr</td></tr>
<tr><td colspan="2">Im Falle spezifischer Risikoelemente (***)</td><td>Verbessert</td><td>Validierungsfunktion AML</td><td>1 Jahr</td></tr>
</table>

(*) Vorausgesetzt, dass der berechnete oder aus der durchgeführten KYC resultierende Risiko-Score mindestens mittel ist. (**) wird auch dann bereitgestellt, wenn definierte Risikoelemente vorhanden sind, die das Risikoprofil unter mittel halten.
(***) auch in Anwesenheit von juristischen Personen mit RP >39 bereitgestellt, wenn sie kommerzielle Aktivitäten im Zusammenhang mit Goldkauf, Glücksspiel und Wetten sowie Abfallsammlung und -entsorgung durchführen (ATECO-Codes mit hohem Risiko) und/oder wenn sie Audits/Untersuchungen unterliegen.

3.4 - WERKZEUGE ZUR UNTERSTÜTZUNG DER DUE DILIGENCE

Das Unternehmen hat neben den bereits verwendeten herkömmlichen Anwendungen technologisch fortschrittliche Tools zur Unterstützung von Prozessen zur Bekämpfung der Geldwäsche implementiert:

- Robotic Process Automation (RPA) wird auf Datenerfassungsaktivitäten in den Bereichen Kunden-Due-Diligence und Meldung verdächtiger Transaktionen angewendet;
- Engine für künstliche Intelligenz, basierend auf statistischen Komponenten und Vorhersageindikatoren (Predict Index AML, Reputational Index und Criminal Infiltration Index), erstellt mit Data Analytics-Techniken, angewendet auf den regulären Kundenbewertungsprozess;
- Cogito-Intelligence-Plattform, eine Anwendung zum Sammeln von Nachrichten, Dokumenten und Textinformationen, um nach negativen Nachrichten über Kunden zu suchen, die einer Due-Diligence-Prüfung unterliegen;

- Rozes, ein Data-Intelligence-Tool, das durch die Analyse von Finanzberichten in Echtzeit die Identifizierung von Unternehmen ermöglicht, deren Bilanz- und Finanzkennzahlen denen von Unternehmen ähneln, die Opfer krimineller Unterwanderung sind.

Darüber hinaus wurden im Rahmen der oben genannten fortschrittlichen Tools bestimmte „Trigger-Ereignisse" identifiziert, die darauf abzielen, Ereignisse in Bezug auf den Kunden und/oder damit verbundene Beziehungen abzufangen und eine Änderung des Ablaufdatums der „Kundenbewertung – KYC" festzulegen, z. B.:

- bei Änderungen der Registerdaten des wirtschaftlich Berechtigten und gesetzlichen Vertreters;
- im Falle einer Änderung des Risikoprofils aufgrund des Vorhandenseins bestimmter Hochrisikofaktoren unter den in der Bestimmung vorgesehenen Faktoren;
- im Falle der Übernahme der Rolle eines PEP durch einen wirtschaftlichen Eigentümer oder der Registrierung eines neuen PEP-wirtschaftlichen Eigentümers;
- im Falle der Delegation an eine natürliche Person wird ein Kundenverhältnis an eine als PEP eingestufte Person übertragen;
- im Falle einer Diskrepanz zwischen dem im Register eingetragenen wirtschaftlichen Eigentümer und den aus den Auszügen der Handelskammer entnommenen Beweisen;
- im Falle von Kontrollen der zweiten Ebene durch die AML-Funktion.

Die Verantwortung für den Due-Diligence-Prozess eines Kunden liegt bei der Relationship-Management-Einheit des Kunden, die sich in der Regel um den Aufbau neuer laufender Beziehungen kümmert, gelegentliche Transaktionen durchführt, bestehende Kunden regelmäßig neu bewertet und eine kontinuierliche Überwachung der Kundenbeziehung gewährleistet.

3.5 - VERPFLICHTUNGEN ZUR ENTHALTUNG

Das Unternehmen verzichtet auf die Aufnahme, Durchführung oder Fortführung der Beziehung, des Geschäftsbetriebs und der professionellen Dienstleistungen (sog. Abstinenzpflicht), wenn eine objektive Unmöglichkeit besteht, eine Kunden-Due-Diligence-Prüfung durchzuführen und zu beurteilen, ob eine verdächtige Transaktion der FIU gemeldet werden soll.

In den Fällen, in denen eine Enthaltung nicht möglich ist, weil eine gesetzliche Verpflichtung zur Durchführung des Vorgangs besteht, die nicht aufgeschoben werden kann, oder wenn eine Ablehnung die Untersuchung behindern könnte, ist das Unternehmen dennoch verpflichtet, die verdächtige Transaktion unverzüglich zu melden.

Darüber hinaus behält sich das Unternehmen das Recht vor, die Geschäftsbeziehung mit dem Kunden einzuschränken oder zu beenden, wenn sich nach einer weiteren Bewertung oder im Anschluss an den erweiterten Due-Diligence-Prozess Elemente mit hohem Risiko ergeben, die das rechtliche und/oder den Ruf des Unternehmens beeinträchtigen könnten. Diese Einschränkungen können sich beispielsweise auf den Zugang des Kunden zu bestimmten Arten von Produkten auswirken oder zur Unterbrechung der vom Unternehmen im Zusammenhang mit dem Konto/der Beziehung angebotenen Dienste führen.

Die von der Gesellschaft ergriffenen Maßnahmen zur Sorgfaltspflicht gegenüber Kunden schließen bzw. verweigern jedoch nicht den Zugang zu Finanzdienstleistungen für Kunden oder ganze Kategorien von Hochrisikokunden, die gemäß der geltenden Gesetzgebung Anspruch

darauf hätten, außer in den Fällen, die im Gesetzesdekret 231/07 ausdrücklich vorgesehen sind und das Verbot der Aufrechterhaltung von Beziehungen zu bestimmten Arten von Unternehmen betreffen.

Das Unternehmen geht keine Korrespondenzbeziehung mit einer Mantelbank ein und unterlässt es, Beziehungen mit Unternehmen einzugehen, die den Zugang zu Korrespondenzbeziehungen zu einer Mantelbank ermöglichen. Es darf keine Geschäftsbeziehung mit Unternehmen eingehen, deren Eigentumsstruktur (Unternehmen, Steuern und Finanzen) durch ein hohes Maß an Undurchsichtigkeit gekennzeichnet ist, die eine eindeutige Identifizierung des wirtschaftlichen Eigentümers oder der Art und des Zwecks der Struktur verhindert.

Zu diesem Zweck ergreift das Unternehmen alle Maßnahmen, um sicherzustellen, dass es nicht absichtlich und wissentlich mit Finanzinstituten zusammenarbeitet, die ihrerseits mit Briefkastenbanken zusammenarbeiten.

Darüber hinaus verzichtet das Unternehmen darauf, eine Geschäftsbeziehung mit Personen einzugehen oder fortzusetzen, die einem besonderen Risiko der Geldwäsche/Terrorismusfinanzierung ausgesetzt sind, wie zum Beispiel:

- Treuhandgesellschaften, die ihren Sitz in einem Land haben, das nach Angaben der FATF einem höheren Geldwäscherisiko ausgesetzt ist oder die keine Maßnahmen ergreifen, die mit den durch das Gesetzesdekret 231/07 oder europäischen Richtlinien auferlegten Verpflichtungen im Einklang stehen;
- Trusts, für die keine angemessenen, genauen und aktuellen Informationen über das wirtschaftliche Eigentum des Trusts sowie seine Art und seinen Zweck verfügbar sind;
- Wettunternehmen, einschließlich Betreiber von Online-Glücksspielen, Casinos und Bingo, für die keine nach italienischem und internationalem Recht erforderliche Genehmigung und/oder Lizenz erteilt und/oder überprüft wurde;
- Verbundene Unternehmen und Vertreter von Zahlungsdienstleistern (im Sinne der Definition von Art. 1 c. 2 Buchstabe nn) und E-Geld-Institute, die die Bestimmungen von Kapitel V des Gesetzesdekrets 231/07 in den Artikeln 43 ff. nicht einhalten;
- Gesellschaften mit beschränkter Haftung oder Gesellschaften, die durch Inhaberaktien kontrolliert werden und ihren Hauptsitz in Ländern mit hohem Risiko haben;
- Kunden, die in der Produktion und im Verkauf von leichtem Marihuana oder in Unterhaltungsstätten für Erwachsene tätig sind, wenn sie nicht in der Lage sind, die gesetzlich erforderlichen Genehmigungen zu überprüfen.

Das Unternehmen verwendet alle im Due-Diligence-Prozess gewonnenen Informationen über seine Kunden und deren Transaktionen, um festzustellen, ob eine Transaktion oder Geschäftsbeziehung direkt oder indirekt mit Personen oder Organisationen in Verbindung steht, die an Geldwäsche, Terrorismusfinanzierung oder der Entwicklung von Massenvernichtungswaffen beteiligt sind, und unterstützt in keiner Weise Transaktionen mit Waffen, die umstritten und/oder durch internationale Verträge verboten sind.
z.B. nukleare, biologische und chemische Waffen, Streubomben, Waffen mit abgereichertem Uran, Antipersonenminen.

Im Hinblick auf die Produktion, den Transport und/oder die Vermarktung anderer als der oben genannten Rüstungsmaterialien kann das Unternehmen Transaktionen unterstützen, die von den zuständigen Behörden ordnungsgemäß genehmigt wurden und mit der geltenden und aktuellen Gesetzgebung vereinbar sind.

3.6 – MELDUNG VERDÄCHTIGER TRANSAKTIONEN

Wann immer das Unternehmen den Verdacht hat oder berechtigte Gründe für den Verdacht hat, dass eine Geldwäsche- oder Terrorismusfinanzierungsoperation durchgeführt oder versucht wurde:

- es übermittelt der Financial Intelligence Unit (FIU) eine verdächtige Transaktionsmeldung, wenn die Transaktion in Italien erfolgt;

- Wenn die Transaktion ihren Sitz in einem anderen Land hat, muss sie den Bestimmungen der lokalen Gesetzgebung entsprechen und, wenn diese die Anwendung von Maßnahmen vorsieht, die denen des EU-Rechts gleichwertig sind, unverzüglich den Leiter der Geldwäschebekämpfung informieren und dabei alle notwendigen Vorkehrungen treffen, um die Identität der Personen zu schützen, die die verdächtige Transaktion melden.

Das Unternehmen hat Verfahren und Prozesse zur Überwachung, Identifizierung und Meldung verdächtiger Aktivitäten gemäß den nach geltendem Recht erforderlichen Zeitvorgaben und Methoden eingeführt.

Mitarbeiter melden unverzüglich jede Kenntnis oder jeden Verdacht auf Geldwäsche, Terrorismusfinanzierung oder andere kriminelle Aktivitäten oder Erträge aus kriminellen Aktivitäten, unabhängig von ihrer Größe, in Übereinstimmung mit dem aktualisierten Organisationsmodell und den Betriebsmodi, die in der Referenz-internen Regelung vorgesehen sind. Bis zum Abschluss des Meldeverfahrens sieht das Unternehmen von der Ausführung der Transaktion ab, es sei denn, dies ist unmöglich, weil eine gesetzliche Verpflichtung zur Annahme der Urkunde besteht oder die Ausführung der Transaktion aufgrund des normalen Geschäftsablaufs nicht aufgeschoben werden kann oder die Ermittlungen behindern könnte. In diesen Fällen erfolgt die Meldung unmittelbar nach Durchführung der Transaktion.

Als Verdachtsgründe gelten die Merkmale, der Umfang und die Art der Transaktion, der Versuch einer Aufspaltung der Transaktion sowie alle sonstigen Umstände, die den Mitarbeitern im Rahmen ihrer Tätigkeit bekannt werden, unter Berücksichtigung des finanziellen Umfangs und der Art der vom Subjekt der verdächtigen Transaktion ausgeübten Tätigkeit auf der Grundlage der im Rahmen der Anti-Geldwäsche-Gesetzgebung erlangten Informationen (z. B. im Rahmen einer Due Diligence).

Um das Risiko einer – auch unbeabsichtigten – Beteiligung des Unternehmens an den oben genannten illegalen Aktivitäten zu begrenzen, wird bei Geldtransfervereinbarungen ein verstärkter Due-Diligence-Prozess aktiviert, bei dem die an dieser Art von Transaktion beteiligten Akteure (Originator, Begünstigter, an der Geldtransfer beteiligte Banken) den Verdacht auf Geldwäsche, Terrorismusfinanzierung oder Verstöße gegen geltende internationale Beschränkungen für bestimmte Waren, Personen oder Organisationen erwecken können.

Nach dem Meldeprozess kann das Unternehmen die Geschäftsbeziehung mit Kunden einschränken und/oder unterbrechen, insbesondere wenn diese Beziehung ein erhebliches Rechts- oder Reputationsrisiko für Rox Pay S.r.l. darstellen könnte.

3.7 – DATENSPEICHERUNG

Das Unternehmen bewahrt alle Dokumente auf und zeichnet alle im Rahmen des Kunden-Due-Diligence-Prozesses erhaltenen Daten auf, um die Rückverfolgbarkeit von Kundentransaktionen sicherzustellen und die Kontrollfunktionen der Bank von Italien und der FIU, einschließlich Inspektionen, zu erleichtern.

Zu diesem Zweck richtete Rox Pay S.r.l. als Finanzintermediär mit Sitz in Italien ein einheitliches elektronisches Archiv (Archivio Unico Informatico oder AUI) ein, das es ihm ermöglicht, Informationen an die Bank von Italien und die FIU gemäß den in Anhang 2 der Bestimmungen zur Datenspeicherung festgelegten technischen Standards bereitzustellen. In

diesem Archiv werden alle Identifikationsdaten und sonstigen Informationen im Zusammenhang mit laufenden Geschäftsbeziehungen und Kundentransaktionen gemäß den geltenden Gesetzen elektronisch gespeichert.

In diesem Zusammenhang hat das Unternehmen als Reaktion auf die jüngsten Aktualisierungen, die durch die „Bestimmungen zur Datenaufbewahrung und zum Zugriff auf Dokumente, Daten und Informationen" und die „Bestimmungen zur aggregierten Datenübertragung" eingeführt wurden, beschlossen, bestimmte Grundsätze für die Befreiung von Registrierungspflichten zu übernehmen, wie ausdrücklich vorgesehen. Insbesondere Daten und Informationen über von Bank- und Finanzintermediären vermittelte Transaktionen, die unter die in Artikel genannten Fälle fallen

8 der Bestimmungen zur Datenspeicherung und Artikel 3 der Bestimmungen zu aggregierten Daten werden nicht im Einheitlichen Elektronischen Archiv erfasst.

Im Hinblick auf die Sorgfaltspflicht gegenüber Kunden bewahrt das Unternehmen Kopien oder Aufzeichnungen aller erforderlichen Dokumente für einen Zeitraum von zehn Jahren nach Beendigung der Geschäftsbeziehung auf.

Bei Transaktionen und laufenden Geschäftsbeziehungen werden alle belegenden Belege und Aufzeichnungen, z. B. Originaldokumente oder gerichtlich zulässige Kopien, für die Dauer von zehn Jahren nach Durchführung der Transaktion bzw. nach Beendigung der Geschäftsbeziehung aufbewahrt.

3.8 – PRÄVENTION REGARGIN RESTRIKTIVE MASSNAHMEN

Aufgrund der Art, Größe und Komplexität seines Geschäfts sowie des Umfangs und der Art der erbrachten Dienstleistungen ist das Unternehmen dem Risiko ausgesetzt, gegen restriktive Maßnahmen zu verstoßen.

Um ein organisatorisches und verfahrenstechnisches System aufrechtzuerhalten, das darauf abzielt, die Einhaltung restriktiver EU-Maßnahmen und nationaler internationaler Maßnahmen sicherzustellen, wird das Risiko von Verstößen gegen restriktive Maßnahmen von der Anti-Geldwäsche-Funktion auf der Grundlage von geografischen Faktoren, Kunden, Produkten/Dienstleistungen und Vertriebskanalfaktoren bewertet. Dabei wird eine ständige Überwachung der Wirksamkeit des Systems gewährleistet, die auch durch die regelmäßige Durchführung einer Selbstbewertung gewährleistet wird, die die Identifizierung etwaiger Korrekturmaßnahmen als Reaktion auf die Erkennung bestehender kritischer Probleme und/oder die Einführung geeigneter Risikopräventionsmaßnahmen ermöglicht Abhilfemaßnahmen.

Das Unternehmen hat Verfahren und Prozesse eingerichtet, um Aktivitäten, die gegen restriktive Maßnahmen verstoßen, zu überwachen, zu identifizieren und zu melden, wobei die Zeitvorgaben und Methoden den gesetzlichen Anforderungen entsprechen.

Die bestehenden Kontrollen von Einzelpersonen/Organisationen und Transaktionen werden durch einen automatisierten Screening-Prozess durchgeführt, der sowohl täglich als auch während der Onboarding-Phase durchgeführt wird, indem spezifische, zweimal täglich aktualisierte Listen zu Kunden, Gegenparteien, Ländern und Transaktionen verwendet werden.

Es sind Prozesse vorhanden, um eingehende oder ausgehende Ströme mit Ländern und/oder Unternehmen zu überwachen, die internationalen Finanzsanktionen unterliegen, wobei die Verantwortlichkeiten zwischen den zuständigen Abteilungen festgelegt werden.

Es wird sichergestellt, dass das Personal angemessen geschult und über die Richtlinien, Verfahren und Kontrollen informiert wird, um restriktive Maßnahmen einzuhalten.

4 – LISTE DER SCHLÜSSELPROZESSE

4.1 – RISIKOMANAGEMENT VON GELDWÄSCHE UND TERRORISTISCHER FINANZIERUNG

Der Prozess „Risikomanagement bei Geldwäsche und Terrorismusfinanzierung" ist der Prozess, mit dem die folgenden Aktivitäten innerhalb des Unternehmens durchgeführt werden, um das Risiko der Nichteinhaltung der Anforderungen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung zu mindern:

- Ermittlung des Risikos der Nichteinhaltung von AML-CFT-Anforderungen durch kontinuierliche Überwachung von Gesetzesänderungen und Bewertung der Auswirkungen auf Geschäftsprozesse und -verfahren sowie Identifizierung und Bewertung von AML-CFT-Risiken mithilfe eines risikobasierten Ansatzes;

- Management und Eindämmung des Geldwäsche- und Terrorismusfinanzierungsrisikos durch Umsetzung und Überwachung von Maßnahmen zur Risikominderung bei Nichteinhaltung, die im Jahresplan (AML-Plan) festgelegt oder von der Unternehmensleitung festgelegt wurden und von allen relevanten Geschäftsfunktionen bei der Umsetzung von Verfahren (interne Vorschriften, IT-Anwendungen, betriebliche Prozesse, Kontrollen) angewendet werden;
- Compliance-Prüfungen (ex-ante und ex-post) in den vom Eigentümer zugewiesenen Regulierungsbereichen durch Definition und Überwachung von Risikoindikatoren und deren Entwicklung im Zeitverlauf. Ziel ist es, mögliche Nichteinhaltungssituationen zu finden und die Ex-ante- und Ex-post-Kontrollaktivitäten durchzuführen;
- Bereitstellung von Beratung und Unterstützung in Fragen der Bekämpfung von Geldwäsche und Terrorismusfinanzierung, Teilnahme an funktionsübergreifenden Arbeitsteams und Unterstützung entweder der Geschäftsstrukturen oder der obersten Führungsgremien in Geschäftsfragen und -prozessen, bei denen das Risiko von Geldwäsche und Terrorismusfinanzierung relevant ist, indem die in den Aufsichtsvorschriften vorgesehenen Erfüllungen durchgeführt werden und eine vorläufige Konformitätsbewertung in diesem Bereich durchgeführt wird, wenn neue Produkte/Dienstleistungen angeboten werden;
- Überwachung und Kontrolle des AML/CFT-Risikos durch Analyse der von Level I und anderen Kontrollfunktionen im Zusammenhang mit betrieblichen Anforderungen zur Bekämpfung der Geldwäsche erhaltenen Informationsflüsse sowie durch Implementierung von Risikoüberwachungskontrollen und ständige Überprüfung ihrer Angemessenheit;
- Durchführung einer AML-Selbstbewertung durch Durchführung vorläufiger Aktivitäten, die zum Ausfüllen der sogenannten „System"- und „Betriebs"-Fragebögen sowie zur Bestimmung des Restrisikos erforderlich sind;
- Berichterstattung an die obersten Unternehmensorgane und Aufsichtsbehörden, insbesondere Vorbereitung der jährlichen Berichterstattung an die Unternehmensorgane und den Aufsichtsrat sowie Vorbereitung der regelmäßigen Berichterstattung über die durchgeführten Aktivitäten und etwaige spezifische Anfragen der Aufsichtsbehörden;
- Bereitstellung spezifischer AML/CFT-Schulungen durch Organisation eines geeigneten Schulungsplans zusammen mit den anderen für die Schulung verantwortlichen Unternehmensfunktionen. Ziel ist eine kontinuierliche Schulung der Mitarbeiter und Mitarbeiter.

Die spezifischen Regeln und Verantwortlichkeiten des Unternehmens in Bezug auf diesen Prozess sind im internen Dokument aufgeführt
Dokument „Interne Verfahren zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung".

4.2 – VERWALTUNG DER BEZIEHUNGEN ZU AUFSICHTSBEHÖRDEN ZUR BEKÄMPFUNG VON GELDWÄSCHE UND TERRORISMUSFINANZIERUNG

Der AML/CFT Regulatory Relationship Management-Prozess ist der Prozess, mit dem Aktivitäten innerhalb des Unternehmens durchgeführt werden, um die gesamte Kommunikation mit Aufsichtsbehörden zu Angelegenheiten im Zusammenhang mit der Bekämpfung von Geldwäsche und Terrorismusfinanzierung zu verwalten, zu analysieren, zu steuern und zu überwachen. Ziel ist die Überwachung dieser Aktivitäten, einschließlich der Archivierung von Dokumenten in einem einzigen Repository.

Im Rahmen dieses Prozesses werden folgende Tätigkeiten durchgeführt:

- Verwaltung der Beziehungen zu Aufsichtsbehörden (Geldwäschebekämpfung), Verwaltung, Analyse und Bearbeitung von Mitteilungen und Anfragen von Aufsichtsbehörden bezüglich der Konformität in diesem Bereich;
- Verwaltung von Aufsichtsberichten zur Bekämpfung der Geldwäsche, durch Vorbereitung des Ablaufs und Versenden von Aufsichtsberichten zur Bekämpfung der Geldwäsche;

- Bearbeitung von Verwaltungsverfahren im Zusammenhang mit der Bekämpfung von Geldwäsche durch Prüfung von Widerklagen im Zusammenhang mit Verwaltungsverfahren, die dem Unternehmen von den zuständigen Behörden (GdF und FIU) mitgeteilt wurden, sowie Vertretung des Unternehmens vor dem MEF, indem er in Abstimmung mit der Budgetfunktion für die Verfahrenszählung im entsprechenden Antrag und für die Zuweisung zur Rückstellung für Risiken und Gebühren und mögliche Sanktionszahlungen verantwortlich ist.

Die spezifischen Regeln und Verantwortlichkeiten des Unternehmens in Bezug auf diesen Prozess sind im internen Dokument „Interne Verfahren zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung" detailliert beschrieben.

4.3 – MANAGEMENT DER OPERATIVEN ANFORDERUNGEN ZUR BEKÄMPFUNG VON GELDWÄSCHE UND TERRORISMUSFINANZIERUNG

Der AML/CFT-Operational-Requirement-Management-Prozess ist der Prozess, mit dem die folgenden Aktivitäten innerhalb des Unternehmens durchgeführt werden, um regulatorische Anforderungen einzuhalten:

- Beschränkung der Verwendung von Bargeld und Inhaberpapieren durch Umsetzung regulatorischer Anforderungen hinsichtlich der Beschränkungen der Verwendung von Bargeld und Inhaberschuldverschreibungen/Wertpapieren;
- Verwaltung angemessener Kunden-Due-Diligence-Verpflichtungen durch Durchführung der Aktivitäten der Kunden-Due-Diligence (oder verstärkter Due-Diligence) in den durch das italienische Gesetz (Gesetzesdekret 231/07 und spätere Änderungen) festgelegten Fällen in Abhängigkeit vom Risikoprofil der Kunden, Unterstützung des Netzwerks des Unternehmens bei der Erfüllung der Verpflichtungen, die durch geltende Gesetze und Vorschriften erforderlich sind, und Bereitstellung von Unterstützung für die Strukturen des Unternehmens, die Beziehungen zu Kunden sowie Bank- und Finanzgegenparteien verwalten, um den Aufbau und die Pflege von Beziehungen zu ermöglichen;
- Verwaltung der Pflichten zur Meldung verdächtiger Transaktionen durch Durchführung der Meldepflichten bei verdächtigen Transaktionen durch Ausführung der Befugnisübertragungen des Verwaltungsrats (ex Art. 36 Gesetzesdekret 231/07) und Überwachung der von der FIU eingegangenen Anfragen;
- Verwaltung der Verpflichtungen im Zusammenhang mit der Bekämpfung der Terrorismusfinanzierung durch Festlegung der Überprüfungsmethodik zur Sicherstellung der Umsetzung restriktiver Maßnahmen der Union und der Mitgliedstaaten, Überprüfung der Umsetzung von Aktualisierungen der Sanktionslisten sowie Berichterstattung an die zuständigen Behörden (nationale und Aufsichtsbehörden) über restriktive Maßnahmen (FIU, MAECI und MEF) zu Maßnahmen zum Einfrieren von Kapital (ex-gesetzesvertretendes Dekret 109/07) und Durchführung der erforderlichen Betriebsanforderungen;
- Verwaltung der Datenaufbewahrungspflichten durch Überprüfung der Zuverlässigkeit des Informationssystems durch Aktualisierung des Archivio Unico Informatico (AUI), Vornahme etwaiger Überarbeitungen, regelmäßige Übermittlung aggregierter Daten an die FIU und Übermittlung der gemäß den Vorschriften erforderlichen Meldungen an die FIU und die Bank von Italien;
- Überwachung der ordnungsgemäßen Umsetzung internationaler Finanzsanktionen (Finanzembargos);

- Kontinuierliche Überwachung von Kunden mit dem höchsten Risiko für Geldwäsche und Terrorismusfinanzierung, Überwachung von Anfragen zur weiteren Untersuchung von Kunden, die das Unternehmen möglicherweise einem hohen Geldwäscherisiko aussetzen, Aktivierung, sofern erforderlich, des Prozesses zur Bewertung verdächtiger Transaktionen und des Prozesses zur Überprüfung von Kunden, die das Unternehmen möglicherweise einem hohen Geldwäscherisiko aussetzen.

Die spezifischen Regeln und Verantwortlichkeiten des Unternehmens in Bezug auf diesen Prozess sind im internen Dokument aufgeführt

Dokument „Interne Verfahren zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung".

5 - ORGANISATORISCHER RAHMEN UND KONTROLLSTELLEN

Um das Risiko von Geldwäsche und Terrorismusfinanzierung sowie von Verstößen gegen die restriktiven Maßnahmen effektiv zu bewältigen, hat das Unternehmen die organisatorischen Funktionen, Ressourcen und Verfahren identifiziert, die mit der Art und dem Umfang der durchgeführten Aktivitäten, der organisatorischen Komplexität sowie den betrieblichen Merkmalen im Einklang stehen und in einem angemessenen Verhältnis dazu stehen.

Die Überwachung von Risiken im Zusammenhang mit Geldwäsche und Terrorismusfinanzierung ist gewährleistet:

- durch die Anti-Geldwäsche-Funktion von Rox Pay S.r.l., deren Verantwortung dem Leiter der AML-Funktion übertragen wird, der direkt dem Chief Executive Officer unterstellt ist.
- Durch das für die Bekämpfung der Geldwäsche zuständige Mitglied des Leitungsorgans, dessen Verantwortung dem CEO übertragen wird. Dieser ist der Hauptkontaktpunkt zwischen dem Leiter der Funktion zur Bekämpfung der Geldwäsche und dem Vorstand und stellt sicher, dass der Vorstand über die notwendigen Informationen verfügt, um die Relevanz der Geldwäscherisiken, denen Rox Pay S.r.l. ausgesetzt ist, vollständig zu verstehen. ist ausgesetzt.

Die Überwachung von Risiken im Zusammenhang mit der Verletzung restriktiver Maßnahmen:

- wird durch den für restriktive Maßnahmen zuständigen leitenden Mitarbeiter sichergestellt, dessen Verantwortung dem Leiter der AML-Abteilung zugewiesen ist, der die Angemessenheit und Wirksamkeit von Richtlinien, internen Verfahren und Kontrollen im Zusammenhang mit der Verwaltung restriktiver Maßnahmen, Sanktionen und Embargos überwacht. Der leitende Mitarbeiter schlägt in Zusammenarbeit mit den zuständigen Unternehmensfunktionen organisatorische und verfahrenstechnische Änderungen vor, die erforderlich und/oder angemessen sind, um eine angemessene Überwachung des Risikos von Verstößen gegen restriktive Maßnahmen, Sanktionen und Embargos sicherzustellen.

In Übereinstimmung mit den geltenden Vorschriften hat die Gesellschaft ihre Organisationsstruktur und Corporate Governance so gestaltet, dass sie die Interessen der Gesellschaft schützt und gleichzeitig eine solide und umsichtige Geschäftsführung gewährleistet und das Risiko – auch wenn es unbeabsichtigt ist – vermeidet
- jegliche direkte Beteiligung an Geldwäsche- und/oder Terrorismusfinanzierungshandlungen.

Zu diesem Zweck sind der Vorstand und die Abschlussprüfer im Einklang mit dem von der Gesellschaft eingeführten internen Kontrollsystem durch klar definierte Aufgaben und Verantwortlichkeiten an der Minderung der oben genannten Risiken beteiligt.

Darüber hinaus hat das Unternehmen eine zentrale Einheit für die Verwaltung des internen Meldesystems für Verstöße eingerichtet, deren Aufgabe es ist, die Aktivitäten zur Entgegennahme, Analyse und Auswertung von Meldungen zu überwachen, die von Mitarbeitern im Rahmen des Whistleblowing-Verfahrens weitergeleitet werden.

6 – ÜBERARBEITUNG UND AKTUALISIERUNG DER RICHTLINIE

Die Anti-Geldwäsche-Funktion überprüft die Richtlinie mindestens einmal jährlich, aktualisiert sie bei Bedarf und bereitet den Text zur Genehmigung durch den Verwaltungsrat auf Vorschlag des Chief Executive Officer vor.

Alle vom Vorstand von Rox Pay S.r.l. genehmigten Änderungen der Richtlinie. werden anschließend unternehmensweit durch Beschluss der Geschäftsleitung umgesetzt und dabei Verantwortlichkeiten, Prozesse und interne Regeln aufeinander abgestimmt.