



**Projekt „Instrument für technische Unterstützung“ (TSI)
„Regionale und lokale Gebietskörperschaften – Verbesserung der Qualität der
öffentlichen Verwaltung und Zusammenarbeit, Verhinderung von Geldwäsche und
Terrorismusfinanzierung in Österreich“**

**Handbuch zur risikobasierten Bekämpfung von Geldwäsche und
Terrorismusfinanzierung für die Verpflichteten gemäß der Gewerbeordnung 1994**

Bearbeitet von:
Maud Bökkerink
Sachverständige des Europarates

Im Rahmen der Mittelausstattung des Instruments für technische Unterstützung des Europarats und der Europäischen Union für 2023 unterstützt die Abteilung Wirtschaftskriminalität und Zusammenarbeit die österreichischen Behörden bei der Stärkung der risikobasierten Überwachung zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung (AML/CFT) in den österreichischen Bundesländern im Einklang mit den Anforderungen der EU und der internationalen (FATF) in Bezug auf die Sektoren, die höheren Risiken in Bezug auf Geldwäsche und Terrorismusfinanzierung ausgesetzt sind. Das Projekt begann am 1. September 2023 und wird 24 Monate dauern.

Durch maßgeschneiderte Aktivitäten soll das Projekt zu Folgendem beitragen:

- Verbesserung der risikobasierten AML/CFT-Beaufsichtigung ausgewählter Sektoren mit höherem Risiko von Verpflichteten, die von den zuständigen regionalen und lokalen Behörden in den österreichischen Bundesländern beaufsichtigt werden;
- Stärkung der interinstitutionellen Zusammenarbeit und des Informationsaustauschs für die Zwecke der AML/CFT-Beaufsichtigung in den österreichischen Bundesländern;
- Verbesserung des Verständnisses der Verpflichteten in Sektoren mit höherem Risiko in Bezug auf ihre AML/CFT-Verpflichtungen.

Besondere Schwerpunkte liegen auf der Überprüfung des bestehenden Rechts- und Verwaltungsrahmens für die risikobasierte AML/CFT-Überwachung von Verpflichteten in ausgewählten Sektoren mit höherem Risiko, die in den Zuständigkeitsbereich der regionalen und lokalen zuständigen Behörden in den österreichischen Bundesländern fallen; Ausarbeitung eines Aktionsplans zur Behebung der festgestellten Mängel bei der risikobasierten AML/CFT Beaufsichtigung sowie bei der interinstitutionellen Zusammenarbeit und dem Informationsaustausch im Inland und innerhalb der EU; die Entwicklung eines einheitlichen Handbuchs für die risikobasierte AML/CFT-Beaufsichtigung für die zuständigen Aufsichtsbehörden in den österreichischen Bundesländern und Leitlinien für die Datenerhebung für die Zwecke der Beaufsichtigung ausgewählter Verpflichteter; Unterstützung bei der Entwicklung eines Rahmens für die Koordinierung und den strukturierten Informationsaustausch zwischen den für AML/CFT zuständigen Aufsichtsbehörden in den österreichischen Bundesländern sowie eines Mechanismus zur Überwachung der Fortschritte und Auswirkungen der AML/CFT-Beaufsichtigung.

Für weitere Informationen wenden Sie sich bitte an:

Abteilung für Wirtschaftskriminalität und Zusammenarbeit (ECCD), Generaldirektion Menschenrechte und Rechtsstaatlichkeit
Europarat – Council of Europe
E-Mail: contact.econcrime@coe.int
Website: www.coe.int/econcrime

Haftungsausschluss:

Dieses Dokument wurde von Experten des Europarates im Rahmen des Projekts TSI - Österreich erstellt.

Die hier dargelegten Ansichten und Meinungen sind die der Autoren und sollten nicht so verstanden werden, dass sie den offiziellen Standpunkt der Europäischen Union und/oder des Europarates widerspiegeln.



INHALTSVERZEICHNIS

VORWORT	6
1 EINFÜHRUNG	7
1.1 Ziel dieses Handbuchs	7
1.2 Bewertung des Geschäftsrisikos	7
1.3 Wie privatwirtschaftliche Rechtsträger dieses Handbuch nutzen sollten	8
2 RISIKOBASIERTER ANSATZ BEI KUNDEN DUE DILIGENCE (CDD)	9
2.1 Risikofaktoren.....	9
2.2 Einbettung des risikobasierten Ansatzes in die Praxis	10
3 KUNDENBEZOGENE SORGFALTSPFLICHTEN (CDD)	10
3.1 Umsetzung der Sorgfaltspflicht gegenüber Kunden	11
3.2 Herkunft der Mittel.....	11
3.3 Beispiele für risikobasierte CDD-Maßnahmen	12
4 ERWEITERTE SORGFALTSPFLICHT (EDD)	12
5 PEP-SCREENING, SANKTIONEN UND NEGATIVE NACHRICHTEN	13
5.1 PEP-Screening.....	13
5.2 Screening auf Sanktionen.....	14
5.3 Screening auf negative Nachrichten.....	14
5.4 Was ist zu tun, wenn eine Übereinstimmung festgestellt wird?.....	15
6 KUNDEN AUS DRITTLÄNDERN MIT HOHEM RISIKO	16
6.1 Ermittlung von Ländern mit hohem Risiko	16
6.2 Konkrete Beispiele	17
7 LAUFENDE ÜBERWACHUNG	17
8 MELDUNG VERDÄCHTIGER TRANSAKTIONEN	18
8.1 GoAML-Zugang.....	19
9 INTERNE MAßNAHMEN ZUR EINHALTUNG DER AML/CFT-VORSCHRIFTEN	19
9.1 Governance	19
9.2 Compliance-Beauftragter oder verantwortliche Person.....	20
9.3 Internes Audit oder unabhängige Überprüfung (proportional zur Größe)	20
9.4 Schulung und Sensibilisierung.....	20
9.5 Negative Berichte	21
10 AUFBEWAHRUNG VON AUFZEICHNUNGEN	21
11 SEKTORSPEZIFISCHE LEITLINIEN	22
11.1 Immobilienmakler.....	22
11.1.1 Fallstudien und Warnsignale.....	23
11.1.2 Risikoindikatoren für Immobilienmakler	26
11.2 Versicherungsvermittler	29



11.2.1 Fallstudien und Warnsignale.....	29
11.2.2 Risikoindikatoren für Versicherungsvermittler	31
11.3 Händler.....	33
11.3.1 Fallstudien und Warnsignale.....	33
11.3.2 Risikoindikatoren für Händler	36
11.4 Unternehmensberater (Unternehmensdienstleister)	38
11.4.1 Fallstudien und Warnsignale.....	38
11.4.2 Risikoindikatoren für Unternehmensberater	42



ABKÜRZUNGEN

AML/CFT	Bekämpfung von Geldwäsche und Terrorismusfinanzierung
CDD	Sorgfaltspflicht gegenüber Kunden (Customer Due Diligence)
EC	Europäische Kommission
EDD	Erweiterte Sorgfaltspflicht (Enhanced Due Diligence)
EU	Europäische Union
FATF	Arbeitsgruppe „Bekämpfung von Geldwäsche und Terrorismusfinanzierung“
FIU	Geldwäschemeldestelle
GewO	Gewerbeordnung
Land (pl. Länder)	Bundesländer der Republik Österreich
GW	Geldwäsche
NRA	Nationale Risikobewertung
OeNB	Österreichische Nationalbank
PEP	Politisch exponierte Person
RBA	Risikobasierter Ansatz
SNRA	Supranationale Risikoanalyse
SOF	Herkunft der Mittel
STR	Meldung verdächtiger Transaktionen
TF	Finanzierung des Terrorismus
TSI	Instrument für technische Unterstützung
WE	Wirtschaftlicher Eigentümer

VORWORT

Dieses Handbuch enthält Leitlinien für die AML/CFT-Verpflichteten (im Folgenden „Rechtsträger“ oder „Unternehmen“ genannt) nach der österreichischen Gewerbeordnung.

Sinn und Zweck dieses Handbuchs ist es, Rechtsträger dabei zu unterstützen, ihre AML/CFT Verpflichtungen nach der Gewerbeordnung zu verstehen und zu erfüllen, und gleichzeitig die Wirksamkeit von Maßnahmen zur Aufdeckung, Verhinderung und Abschreckung von Geldwäsche und Terrorismusfinanzierung zu erhöhen. Das Handbuch dient zur kohärenten und risikosensitiven Anwendung der AML/CFT-Anforderungen in allen relevanten Sektoren.

Dieses Dokument ist in Verbindung mit anderen geltenden Leitlinien der Aufsichtsbehörden sowie einschlägigen EU- und internationalen Standards zu lesen.

Es sei darauf hingewiesen, dass das Handbuch als allgemeiner politischer Rahmen und als Auslegungshilfe dient. Es setzt die rechtlichen Anforderungen der Gewerbeordnung und die damit verbundenen Verordnungen nicht außer Kraft und ersetzt diese auch nicht. Die Rechtsträger müssen sicherstellen, dass ihre Praktiken weiterhin uneingeschränkt mit allen geltenden rechtlichen Verpflichtungen im Einklang stehen, auch wenn sie sich bei der praktischen Umsetzung auf dieses Handbuch stützen.

Mit diesem Handbuch wird ein risikobasierter Ansatz gefördert, der es den Rechtsträgern ermöglicht, ihre AML/CFT Maßnahmen entsprechend der Art und dem Grad des Risikos, mit dem sie es zu tun haben, anzupassen. Ein gut umgesetzter risikobasierter Ansatz fördert die Effizienz und die Priorisierung der Ressourcen, wobei die Fairness und Verhältnismäßigkeit bei der Behandlung von Kunden und Transaktionen gewahrt bleiben. Ziel ist nicht nur die Erfüllung der Compliance-Verpflichtungen, sondern auch die Förderung einer Kultur der Rechtstreue, die sowohl von den Rechtsträgern selbst als auch von der breiten Öffentlichkeit als fair, transparent und ausgewogen wahrgenommen wird.



1 EINFÜHRUNG

1.1 Ziel dieses Handbuchs

Geldwäsche (ML), Terrorismusfinanzierung (TF) und die Umgehung von Sanktionen stellen komplexe und dynamische Bedrohungen in einer Vielzahl von Wirtschaftssektoren in Österreich dar. Die Rolle der nichtfinanziellen Unternehmen und Berufe, insbesondere derjenigen, die unter die österreichische Gewerbeordnung (GewO) fallen, ist bei der Aufdeckung und Verhinderung illegaler Finanzströme zunehmend wichtiger geworden.

Rechtsträger, die unter die GewO fallende Tätigkeiten ausüben, wie Immobilienmakler, Versicherungsvermittler, Händler und Unternehmensberater (Unternehmensdienstleister), unterliegen den Verpflichtungen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung (AML/CFT). Die AML/CFT-Aufsicht dieser Sektoren wird von der zuständigen Behörde in jedem Bundesland wahrgenommen.

Dieses Handbuch soll Immobilienmakler, Versicherungsvermittler, Händler und Unternehmensberater in Österreich mit praktischen und sektorspezifischen Leitlinien unterstützen. Es ergänzt die bestehenden Rechts- und Aufsichtspflichten durch konkrete Beispiele und Risikoindikatoren, wodurch die Lücke zwischen Regulierung und praktischer Umsetzung geschlossen wird.

Diese Leitlinien spiegeln Folgendes wider:

- AML/CFT-Verpflichtungen im Rahmen der GewO
- AML/CFT-Aufsicht durch die Aufsichtsbehörden der Bundesländer
- Meldepflichten gegenüber der zentralen Meldestelle (FIU)
- Praktische Empfehlungen zur Ermittlung und Minderung von ML/TF-Risiken und Sanktionsrisiken.

Das Handbuch enthält auch eine Reihe von (anonymisierten) Fallstudien und Risikoindikatoren. Hierdurch sollen drei Ziele erreicht werden:

Veranschaulichung von echten Situationen, in denen Geldwäsche, Terrorismusfinanzierung oder Verstöße gegen Sanktionen durch Missbrauch legaler Leistungen aufgetreten sind oder hätten auftreten können.

Frühzeitige Erkennung von Warnsignalen bei verdächtigem Verhalten oder ungewöhnlichen Mustern, die möglicherweise nicht immer offensichtlich kriminell erscheinen.

Förderung der Umsetzung verhältnismäßiger und risikobasierter Kontrollen im Einklang mit der nationalen Risikobewertung (NRA) Österreichs und der supranationalen Risikobewertung (SNRA) der EU.

1.2 Bewertung des Geschäftsrisikos

Grundlage jedes internen AML/CFT Rahmens ist eine Bewertung des Geschäftsrisikos. Die Bewertung des Geschäftsrisikos ist eine obligatorische Bewertung auf Ebene der Rechtsträger, die jedes Unternehmen durchführen muss, um das Gesamtrisiko der Geldwäsche und Terrorismusfinanzierung zu verstehen. Bei dieser Bewertung werden Faktoren wie Kundentypen, mit denen das Unternehmen geschäftlich zu tun hat, die Art und die

Komplexität seiner Dienstleistungen, Transaktionen und Produkte sowie die geografischen Gebiete, in denen es tätig ist oder Kundenbeziehungen unterhält, berücksichtigt. Wichtig ist, dass die Bewertung die mit dem Geschäftsmodell selbst verbundenen inhärenten Risiken widerspiegelt.

Die Aufsichtsbehörden haben sektorspezifische Guidance vorbereitet, um die Unternehmen bei der Durchführung ihrer Risikobewertungen zu unterstützen. Die Unternehmen haben damit die Möglichkeit, die Checkliste zur Risikobewertung der Behörden dazu zu verwenden, um ihre eigene Methodologie zur Risikobewertung zu erarbeiten.

Wenn ein Unternehmen sein eigenes Risikoprofil versteht, kann es seine Ressourcen wirksamer einsetzen, interne Kontrollen festlegen und für verhältnismäßige Compliance-Anstrengungen bei allen seinen Tätigkeiten sorgen.

Die Ergebnisse der Bewertung des Geschäftsrisikos müssen direkt in die Gestaltung und Umsetzung der internen Strategien, Verfahren und Maßnahmen des Unternehmens einfließen. Diese internen Maßnahmen wie Risikoeinstufungsmethoden, Kundenakzeptanzstandards und laufende Überwachung sollten auf die ermittelten Risiken zugeschnitten sein. Eine gut kalibrierte Bewertung des Geschäftsrisikos stellt sicher, dass die Maßnahmen zur Erfüllung der Sorgfaltspflichten gegenüber den Kunden (CDD) insgesamt risikosensitiv und einheitlich angewandt werden.

1.3 Wie privatwirtschaftliche Rechtsträger dieses Handbuch nutzen sollten

Dieses Handbuch bietet einen praktischen Rahmen für die Erkennung und Verhinderung von Geldwäsche und Terrorismusfinanzierung und sanktioniert Risiken im Einklang mit den regulatorischen Vorgaben Österreichs im Rahmen der GewO. Durch Umsetzung dieser Maßnahmen halten die Unternehmen nicht nur die Vorschriften ein, sondern tragen auch zur Integrität und Widerstandsfähigkeit der österreichischen Wirtschaft bei.

Dieses Handbuch soll Unternehmen, Compliance-Beauftragten und Führungskräften dabei helfen,

- ihre internen Risikobewertungsprozess zu verbessern, indem sie verstehen, wie ihre Dienstleistungen missbraucht werden können
- interne Strategien und Prozesse, einschließlich der kundenbezogenen Sorgfaltspflichten, laufende Überwachung und Berichterstattung zu aktualisieren oder zu verfeinern
- Personal und Mitarbeiter zu schulen, um Warnsignale und Unstimmigkeiten im Kundenverhalten zu erkennen und zu eskalieren
- einen verhältnismäßigen, risikobasierten Ansatz gemäß den österreichischen AML/CFT-Rechtsvorschriften zu finden.

Die Rechtsträger sollten dieses Papier nicht als Checkliste oder Regelwerk behandeln. Vielmehr sollte es zusammen mit den Rechtsvorschriften und den Leitlinien der österreichischen Behörden und der zentralen Meldestelle als unterstützendes Instrument für die fachliche Einschätzung genutzt werden.

Die Rechtsträger sind aufgefordert,



- die Fallstudien zu überprüfen und mit ihren eigenen Gefährdungs- und Geschäftsmodellen zu vergleichen
- Leitlinien und Risikoindikatoren den bestehenden internen Kontrollen zuzuordnen, um potenzielle Lücken oder Schwachstellen zu ermitteln
- einschlägige Fallstudien in die Schulung des Personals aufzunehmen
- zeitnahe Schritte zur Überprüfung, Eskalation und Meldung an die zentrale Meldestelle zu ergreifen, sollten in der Praxis Warnsignale auftreten.

Das Ziel dieses Handbuches besteht letztlich darin, die Bekämpfung von Geldwäsche und Terrorismusfinanzierung effektiv und praktisch zu fördern, indem österreichische Unternehmen und Fachkräfte anhand von realistischen Beispielen und praktikablen Erkenntnissen geschult werden, die auf ihren jeweiligen Sektor zugeschnitten sind. Damit trägt der Privatsektor unmittelbar zur Wahrung der Integrität der österreichischen Wirtschaft und des EU-Finanzsystems im weiteren Sinne bei.

2 RISIKOBASIERTER ANSATZ BEI KUNDEN DUE DILIGENCE (CDD)

Der risikobasierte Ansatz (RBA) bildet die Grundlage für eine wirksame Einhaltung der Vorschriften zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung. Nach den AML/CFT-Vorschriften wird von Unternehmen nicht erwartet, dass sie alle Kunden und Transaktionen gleich behandeln. Stattdessen müssen sie ML/TF-Risiken je nach Art des Kunden, erbrachter Dienstleistung, geografischem Kontext und ausgeführter Transaktionen angemessen bewerten und behandeln.

In der Praxis bedeutet eine risikosensitive Anwendung der Kundensorgfaltspflichten die Zuweisung von Ressourcen und eine Kontrolle, die dem Risikoniveau angemessen ist. Bei Kunden und Transaktionen, die als risikoarm eingestuft werden, können vereinfachte Maßnahmen angewendet werden. Umgekehrt erfordern risikoreichere Beziehungen oder Verhaltensweisen eine erweiterte Sorgfaltspflicht (EDD) und eine laufende Überwachung.

2.1 Risikofaktoren

Zur risikosensitiven Anwendung der Sorgfaltspflichten gegenüber Kunden sollten Unternehmen zunächst relevante Risikofaktoren vor und während der Begründung der Geschäftsbeziehung bewerten. Dies umfasst:

- **Kundenrisiko:** Handelt es sich bei dem Kunden um eine politisch exponierte Person (PEP)? Handelt der Kunde im Namen einer anderen Person? Sind die Herkunft der Gelder oder Vermögenswerte unklar?
- **Geografisches Risiko:** Sind der Kunde oder sein Geschäft mit einem Drittland mit hohem Risiko verbunden? Besteht ein Zusammenhang mit Jurisdiktionen, die für Korruption, Steuergeheimnisse oder Sanktionen bekannt sind?
- **Produkt-/Dienstleistungsrisiko:** Ist die Erbringung der Dienstleistung anfällig für Missbrauch, z. B. Nominee-Personen, flexible Versicherungsprodukte oder hohe Vermögenswerte?
- **Risiko der Lieferkanäle:** Wird das Onboarding persönlich oder digital durchgeführt? Sind Intermediäre beteiligt, und werden diese beaufsichtigt oder nicht reguliert?



Jeder dieser Faktoren sollte in die Risikobewertung einfließen und den auf die Kunden und auf die jeweilige Situation anzuwendenden Prüfungsgrad bestimmen. Die Umsetzung von CDD-Maßnahmen muss dokumentiert, risikobasiert und dynamisch sein. Dabei handelt es sich nicht um eine Check-the-Box-Übung, sondern um aktive, dynamische Prozesse, die Unternehmen dabei helfen, ihre Aufgaben im Bereich der Bekämpfung von Geldwäsche und Terrorismusfinanzierung zu erfüllen und gleichzeitig ihre Tätigkeiten vor rechtlichen Schäden und Rufschädigung zu schützen.

2.2 Einbettung des risikobasierten Ansatzes in die Praxis

Der risikobasierte Ansatz muss, um wirksam zu sein, in die internen Prozesse und in das Verhalten der Mitarbeiter integriert sein.

Dies bedeutet:

- Entwicklung und Einsatz branchenspezifischer Risikobewertungsinstrumente
- Schulung der Mitarbeiter, um die richtigen Fragen zu stellen und Risiken zu bewerten, und nicht nur Dokumente zu bearbeiten
- Dokumentation, welche Kunden und Situationen als höheres Risiko eingestuft werden und welche Kontrollmaßnahmen dementsprechend angewandt wurden.
- Regelmäßige Überprüfung des Geschäftsrisikos, insbesondere bei Änderungen der Geschäftspraktiken, dem Transaktionsverhalten oder bei externen Ereignissen (z. B. neue Sanktionslisten).

Bei der risikosensitiven Anwendung der kundenbezogenen Sorgfaltspflichten geht es nicht darum, weniger zu tun; es geht darum, das zu tun, was angemessen ist. Unternehmen müssen sich ein Urteil bilden, das sich auf das Gesetz, die Risikotypologien und die Leitlinien der Behörden stützt, um sicherzustellen, dass ihre Präventivmaßnahmen sowohl verhältnismäßig als auch wirksam sind.

3 KUNDENBEZOGENE SORGFALTPFLICHTEN (CDD)

CDD ist ein Eckpfeiler zur wirksamen Einhaltung der AML/CFT-Vorschriften und ist immer dann anzuwenden, wenn eine neue Geschäftsbeziehung begründet wird, eine Transaktion den gesetzlichen Schwellenwert von 10.000 EUR überschreitet, der Verdacht auf Geldwäsche, Terrorismusfinanzierung entsteht oder aufgrund der tatsächlichen Identität des Kunden. Sie dient dem Risikomanagement und muss in den täglichen Betrieb integriert werden.

Die Sorgfaltspflicht gegenüber Kunden ist in folgenden Fällen durchzuführen:

- Bei Begründung einer Geschäftsbeziehung
- Bei Transaktionen von mehr als 10.000 EUR
- Bei Verdacht auf Geldwäsche und Terrorismusfinanzierung
- Bei Zweifeln an der Richtigkeit oder Angemessenheit zuvor erhobener Daten.

Zu den CDD-Schritten gehören:

1. Identifizierung und Überprüfung der Identität des Kunden anhand zuverlässiger Dokumente



2. Identifizierung und Überprüfung des letztendlichen wirtschaftlichen Eigentümers (WE)
3. Verständnis des Zwecks und der beabsichtigten Art der Geschäftsbeziehung
4. Fortlaufende Überwachung der Beziehungen und Transaktionen, gegebenenfalls einschließlich einer Bewertung der Mittelherkunft.

3.1 Umsetzung der Sorgfaltspflicht gegenüber Kunden

Zur ordnungsgemäßen Umsetzung der Sorgfaltspflicht gegenüber Kunden müssen die Unternehmen zunächst die Identität des Kunden anhand zuverlässiger, unabhängiger Quelldokumente wie Pässe oder Personalausweise ermitteln und überprüfen. Hierzu gehören die Erfassung des vollständigen gesetzlichen Namens, Geburtsdatums und -orts, der Staatsangehörigkeit und der Anschrift des Kunden sowie die Aufbewahrung einer lesbaren Kopie des Ausweisdokuments.

Bei juristischen Personen verlangt die Sorgfaltspflicht gegenüber Kunden die Erhebung aktueller Unternehmensaufzeichnungen, wie z. B. einen Auszug aus dem Handelsregister zur Überprüfung der Rechtsform, der Anschrift, der Registrierungsnummer und die Identität des WE.

Die WE müssen anhand von Belegen wie Aktionärsregistern, Treuhandurkunden oder WE-Registern überprüft werden.

Darüber hinaus müssen Unternehmen Informationen über die Art und den Zweck der Geschäftsbeziehung einholen. Bei diesem Schritt geht es oft darum, zu fragen, warum der Kunde die Dienstleistungen in Anspruch nimmt, welche Art von Tätigkeit erwartet und wie die Transaktion finanziert wird.

3.2 Herkunft der Mittel

Händler, die Barzahlungen von mehr als 10.000 EUR akzeptieren, sollten auch eine **Plausibilitätsprüfung** der Geldquelle des Kunden (SOF) durchführen. Ebenso sollten Rechtsträger in Situationen, in denen kein hohes Risiko besteht, sicherstellen, dass die angegebenen SOF angesichts des Profils, der Beschäftigung oder der Geschäftstätigkeit des Kunden angemessen erscheinen. Für solche Plausibilitätsprüfungen reicht es im Allgemeinen, sich auf die Erklärung des Kunden oder eine schriftliche Erklärung zu stützen. Wenn die vorgelegten Informationen jedoch vage oder inkohärent sind oder die SOF nicht hinreichend erläutern, muss der Rechtsträger entsprechende Schritte unternehmen, um weitere Nachweise zu erhalten. Die Intensität dieser Kontrollen sollte in einem angemessenen Verhältnis zu den ermittelten Risiken im Zusammenhang mit der Herkunft der Mittel stehen, aber in jedem Fall sollten die Rechtsträger nachweisen können, dass die SOF bewertet und für glaubwürdig befunden wurde.

Insbesondere bei Situationen oder Transaktionen mit hohem Risiko, z. B. bei Käufen von hohem Wert, komplexer Unternehmensstruktur oder bargeldintensiven Unternehmen, sollte ein Rechtsträger die SOF eingehender bewerten, indem er Nachweise anfordert und die vorgelegten Nachweise aufbewahrt.

Zweck der Bewertung der SOF ist es, zu verstehen, wie das für die Transaktion verwendete Geld erworben wurde und ob es dem Kundenprofil und dem erklärten Zweck entspricht. Informationen über die SOF sollten in verhältnismäßiger und risikobasierter Weise

angefordert werden, wobei offene Fragen und gegebenenfalls dokumentierte Folgemaßnahmen zu verwenden sind.

Zulässige Beweismittel können je nach Kontext Bankauszüge, Gehaltsabrechnungen, Kaufverträge, Steuererklärungen, Erbschaftsdokumente oder Darlehensvereinbarungen sein. Die Informationen sind auf Plausibilität und Kohärenz zu überprüfen. Zum Beispiel ist zu prüfen, ob die angegebene Quelle mit der Beschäftigung oder der Jurisdiktion des Kunden übereinstimmt und ob der Transaktionsbetrag angesichts dieser Informationen angemessen ist. Die Unternehmen sollten sowohl die erhaltenen Informationen als auch die Gründe für ihre Annahme dokumentieren und, wenn Zweifel bestehen oder Unstimmigkeiten auftreten, zur internen Überprüfung eskalieren oder eine Meldung verdächtiger Transaktionen (STR) einreichen.

3.3 Beispiele für risikobasierte CDD-Maßnahmen

In Fällen mit geringem Risiko, wie dem Verkauf einer kleinen Immobilie an einen bekannten inländischen Käufer über eine österreichische Hypothekenbank oder eine einfache Unternehmensberatung eines langjährigen österreichischen Unternehmens, kann das Unternehmen vereinfachte Maßnahmen ergreifen. Dies könnte bedeuten, dass grundlegende Unterlagen akzeptiert, eine einmalige ID-Prüfung durchgeführt und Aktualisierungen nur dann vorgenommen werden, wenn neue Risiken auftreten.

In Fällen mit mittlerem Risiko, z. B. bei Transaktionen, an denen EU-Kunden mit glaubwürdigen Einkommensnachweisen beteiligt sind, oder bei einem einmaligen hohen Verkaufswert, der über eine renommierte Bank in der EU abgewickelt wird, würden die üblichen Standard-Sorgfaltspflichten gegenüber Kunden angewandt (Identifizierung und Überprüfung des Kunden, WE-Überprüfung und Ermittlung der Herkunft der Mittel).

In Situationen mit hohem Risiko, z. B. wenn ein Kunde Intermediäre, komplexe Unternehmensstrukturen oder undurchsichtige ausländische Finanzierungen einsetzt, sollte das Unternehmen seine Kontrollen verstärken. Dies könnte u. a. Folgendes umfassen: Die Anforderung detaillierter Erklärungen und Verträge, die Durchführung weiterer Kontrollen des letztendlichen wirtschaftlichen Eigentümers, die Anforderung einer Genehmigung durch die Geschäftsleitung und die Dokumentation des gesamten Schriftverkehrs, um die Kontrolle über das Risiko nachzuweisen.

4 ERWEITERTE SORGFALTSPFLICHT (EDD)

EDD ist in Situationen mit hohem Risiko erforderlich. EDD geht über CDD hinaus. Wichtig ist es, den Kontext der Beziehung zu verstehen und zusätzliche Prüfungen und Kontrollen durchzuführen, um das erhöhte Risiko abzumindern. EDD ist insbesondere beim Umgang mit Kunden aus Drittländern mit hohem Risiko (laut Definition der Europäischen Kommission), PEPs, ihren direkten Familienangehörigen oder nahestehenden Personen sowie komplexen Eigentumsstrukturen anzuwenden, bei denen die wirtschaftliche Begründung unklar ist.

In der Praxis umfasst EDD mehrere Schritte:

1. Unternehmen sollten detailliertere Hintergrundinformationen über den Kunden einholen, einschließlich der beruflichen oder finanziellen Vorgeschichte, der Geschäftspartner sowie der WE und der Unternehmensstruktur. Diese Informationen



- sollten klar dokumentiert und mit externen Datenquellen wie öffentlichen Registern, Open Source Intelligence oder Wirtschaftsdatenbanken abgeglichen werden.
2. Unternehmen sollten zusätzliche Unterlagen für Transaktionen von hohem Wert oder für den Fall verlangen, dass Alarmsignale auftreten. Wenn beispielsweise ein Immobilienmakler einen Immobilienankauf vermittelt, der von einem ausländischen Unternehmen finanziert wird, wäre es angebracht, Nachweise darüber zu verlangen, wie dieses Unternehmen seine Mittel erhalten hat, wer seine Anteilseigner sind und warum es an der Transaktion beteiligt ist.
 3. Die Aufnahme oder Fortführung von Hochrisiko-Beziehungen sollte von der Geschäftsleitung genehmigt werden. Dies bedeutet, dass zuvor ein Manager oder Compliance-Beauftragter die verfügbaren Informationen überprüfen, das Risikoprofil bewerten und seine Entscheidung dokumentieren muss.
 4. EDD beinhaltet eine häufigere Überwachung. Kunden mit hohem Risiko sollten in kürzeren Zeitabständen überprüft werden, und alle ungewöhnlichen oder komplexen Transaktionen sollten einer genaueren Prüfung unterzogen werden. Treten neue Risiken auf oder verweigert der Kunde die Zusammenarbeit, sollte die Beziehung ausgesetzt und gemeldet werden.

5 PEP-SCREENING, SANKTIONEN UND NEGATIVE NACHRICHTEN

Alle Rechtsträger müssen Kunden, WE und relevante Gegenparteien auf den Status einer politisch exponierten Person (PEP), auf Sanktionsexposition und auf negative Nachrichten überprüfen. Während große Institutionen automatisierte Systeme und Wirtschaftsdatenbanken dazu nutzen, können die meisten kleineren Unternehmen angemessene manuelle Screening-Maßnahmen ergreifen, die dennoch den rechtlichen Anforderungen entsprechen. Auch ohne kommerzielle Software oder große Compliance-Teams können Unternehmen ihren Verpflichtungen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung nachkommen, indem sie verhältnismäßige Überprüfungen durchführen und auf die gewonnenen Erkenntnisse reagieren.

Unternehmen sollten eine klare, kohärente und gut dokumentierte risikobasierte Strategie verfolgen. Dabei geht es nicht um Komplexität, sondern um Kohärenz, Dokumentation und risikobasiertes Urteil.

5.1 PEP-Screening

PEPs sind Personen, die ein wichtiges öffentliches Amt innehaben oder innehatten (z. B. Staatsoberhäupter, Minister, Richter, Militärbeamte, Führungskräfte staatlicher Unternehmen), einschließlich ihrer direkten Familienangehörigen und bekannten Geschäftspartner. PEPs sind keine verbotenen Kunden, aber sie erfordern aufgrund eines höheren Korruptionsrisikos eine erweiterte Sorgfaltspflicht sowie eine verstärkte kontinuierliche Überwachung.

PEP-Screening der Unternehmen:

- Verwenden Sie ein PEP-Formular zur Selbstauskunft oder stellen Sie während des Onboardings die richtigen Fragen: Stellen Sie klar formulierte und gut erläuterte PEP-Fragen in dem Kundenaufnahmeformular: „Sind Sie oder einer der wirtschaftlichen Eigentümer eine PEP oder eng mit einer solchen verbunden?“

zusammen mit einer angemessenen Erläuterung, welche Funktionen und Rollen als PEP einzustufen sind.

- Führen Sie grundlegende Open-Source-Prüfungen durch. Nutzen Sie kostenlose Online-Ressourcen (Google, offizielle Regierungswebseiten, LinkedIn usw.), um zu bestätigen, ob der Kunde oder der WE eine öffentliche Position innehat oder innehatte. Verwenden Sie Begriffe wie: „[Kundenname]“ + „Minister“ ODER „Regierung“ ODER „staatlich“ ODER „Parlament“.
- Konsultieren Sie die österreichischen oder EU-PEP-Listen und -Leitlinien. Die Behörden eines Landes können Leitlinien dazu veröffentlichen, wer als inländische PEP einzustufen ist. Gleichen Sie die Rollen mit der rechtlichen Definition einer PEP ab und wenden Sie, wenn erforderlich, EDD an.
- Dokumentieren Sie das Screening: Bewahren Sie einen Screenshot oder einen kurzen Vermerk in der Datei auf, aus dem hervorgeht, wann und wie das PEP-Screening durchgeführt wurde.

5.2 Screening auf Sanktionen

Das Screening auf Sanktionen ist von entscheidender Bedeutung, um den Umgang mit Personen oder Organisationen zu verhindern, die auf Sanktionslisten der EU, VN oder nationalen Sanktionslisten aufgeführt sind, insbesondere im Zusammenhang mit Terrorismus, Verbreitung von Waffen und ausländischen politischen Zielen (z. B. Russland, Iran).

Wie Unternehmen auf Sanktionen prüfen können:

- Verwenden Sie offizielle Sanktionssuchmaschinen der EU oder der Vereinten Nationen: EU-Sanktionskarte und die konsolidierte Liste der Vereinten Nationen.
- Manuelle Suche nach Namen: Geben Sie vor dem Onboarding den Namen des Kunden und etwaiger WE in die oben genannten Datenbanken ein. Gibt es eine Übereinstimmung, setzen Sie die Transaktion nicht fort.
- Vorsicht bei Jurisdiktionen mit hohem Risiko: Wenn der Kunde oder der WE aus einem Land mit hohem Risiko stammt oder in diesem Land tätig ist, wenden Sie die EDD an.
- Bewahren Sie die Aufzeichnungen auf: Halten Sie das Datum und das Ergebnis jeder Kontrolle fest. Selbst in kleinen Unternehmen ist eine kohärente Dokumentation von großer Bedeutung bei Aufsichtsinspektionen.

5.3 Screening auf negative Nachrichten

Ein Screening auf negative Nachrichten kann helfen, Reputations- und Finanzkriminalitätsrisiken aufzudecken, die möglicherweise noch nicht in Strafregistern oder Sanktionslisten aufgeführt sind.

Ein solches Screening ist nicht in jedem Fall erforderlich, sollte jedoch berücksichtigt werden, wenn es Hinweise auf ein erhöhtes Risiko gibt, z. B. ungewöhnliches Kundenverhalten, komplexe Unternehmensstrukturen oder Unstimmigkeiten in der Dokumentation. In Situationen mit höherem Risiko kann ein Screening auf negative Nachrichten einen wertvollen Kontext bieten und dazu beitragen, bestehende Risikoindikatoren zu untermauern und eine fundiertere Bewertung des Risikoprofils des Kunden zu erhalten. Durch den gezielten Einsatz



negativer Medien-Screenings wird sichergestellt, dass die Sorgfaltspflicht gegenüber Kunden (CDD) verhältnismäßig und risikobasiert ausgeübt wird.

Wie Unternehmen negative Medienkontrollen durchführen können:

- Nutzung von open-source Internetsuchmaschinen: Suche nach dem vollständigen Namen des Kunden und allen bekannten Aliasnamen zusammen mit Schlüsselwörtern wie: „Geldwäsche“, „Betrug“, „Sanktion“, „Korruption“, „strafrechtliche Ermittlungen“, „Scam“ oder „Terrorismusfinanzierung“. Beispiel: „Max Mustermann“ UND „Betrug“ ODER „Korruption“.
- Suche in relevanten Sprachen: Übersetzen Sie die Suchbegriffe, wenn der Kunde ausländische Verbindungen hat. Google Translate kann dabei helfen.
- Regionale Presse und Unternehmensregister: Regionalzeitungen, Wirtschaftskammern und Gerichtsmitteilungen können Informationen über Prozesse, Insolvenzen oder Vollstreckungsmaßnahmen haben.
- Dokumentation und Bewertung der Ergebnisse: Falls negative Nachrichten festgestellt werden, prüfen Sie, ob die Vorwürfe glaubwürdig, aktuell und relevant sind. Tragen Sie die Erkenntnisse in die Kunden-Risikodatei ein und eskalieren Sie diese an das Management.

5.4 Was ist zu tun, wenn eine Übereinstimmung festgestellt wird?

Ergibt das Screening eine bestätigte PEP, eine Übereinstimmung bei Sanktionen oder negativen Nachrichten, die einen Verdacht aufkommen lassen:

- Wenden Sie EDD an: Suche nach detaillierten Informationen über die Mittelherkunft, genauere Überwachung der Transaktionen und Genehmigung der Geschäftsbeziehung durch die Geschäftsleitung.
- Im Falle eines bestätigten Treffers bei Sanktionen oder mutmaßlichen kriminellen Aktivitäten führen Sie die Transaktion oder das Onboarding nicht fort und, soweit möglich, frieren Sie bereits erhaltene Gelder ein und erbringen Sie keine neuen Dienstleistungen.
- Einreichung einer Verdachtsmeldung (STR) bei der zentralen Meldestelle. Informieren Sie den Kunden niemals darüber, dass eine STR eingegangen ist (dies gilt als „Tipping-off“ und ist gesetzlich verboten).

Im Falle eines bestätigten Treffers auf einer Sanktionsliste der EU oder der Vereinten Nationen müssen Unternehmen unverzüglich Maßnahmen im Einklang mit den geltenden Sanktionsvorschriften ergreifen. Dazu gehört, dass keine weiteren Transaktionen durchgeführt oder Kunden aufgenommen, Vermögenswerte oder bereits erhaltene Gelder (soweit möglich) eingefroren werden und die Erbringung weiterer Dienstleistungen verhindert wird.

Es sei darauf hingewiesen, dass ein Treffer auf einer Sanktionsliste nicht mit einer an die zentrale Meldestelle übermittelten STR identisch ist. Stattdessen sind alle bestätigten oder vermuteten Treffer auf einer Sanktionsliste gemäß den österreichischen Sanktionsverfahren **unverzüglich** dem Bundesministerium des Innern und der OeNB zu melden. Die Rechtsträger sollten darauf achten, dass das Personal darin geschult ist, Sanktionsverpflichtungen zu



erkennen und interne Eskalationsprozesse anzuwenden, wenn eine potenzielle Übereinstimmung festgestellt wird.

6 KUNDEN AUS DRITTLÄNDERN MIT HOHEM RISIKO

Die Rechtsträger müssen auf Kunden aus oder verbunden mit Drittländern mit hohem Risiko die erweiterte Sorgfaltspflicht (EDD) anwenden. Dies sind Länder, in deren nationalen Systemen die Europäische Kommission strategische Mängel bei der Bekämpfung von Geldwäsche und Terrorismusfinanzierung feststellte, die eine erhebliche Bedrohung für das Finanzsystem der EU darstellen.

Beim Umgang mit Kunden oder wirtschaftlichen Eigentümern (WE) sowie Transaktionen im Zusammenhang mit einem Drittland mit hohem Risiko müssen folgende verstärkte Maßnahmen angewandt werden:

- Einholung zusätzlicher Informationen über den Kunden und die beabsichtigte Art der Geschäftsbeziehung (z. B. Zuverlässigkeitsüberprüfungen, Dokumentation der Herkunft der Mittel und des Vermögens)
- Häufigere Überprüfung der Geschäftsbeziehung, einschließlich einer Überprüfung der Transaktionsmuster
- Zustimmung bei der Geschäftsleitung, bevor die Geschäftsbeziehung begründet oder fortgesetzt wird
- Verstärkte Überwachung zur Aufdeckung ungewöhnlicher oder verdächtiger Aktivitäten.

Alle Schritte zur Identifizierung, Bewertung und Minderung der Risiken im Zusammenhang mit Hochrisiko-Drittländern müssen klar dokumentiert werden. Dies umfasst:

- Für die Länderklassifikation verwendete Quellenlisten
- Interne Memos oder Vermerke zur Risikobewertung
- CDD/EDD-Checklisten und Genehmigungen
- Kopien der erhaltenen Dokumente.

6.1 Ermittlung von Ländern mit hohem Risiko

Die Europäische Kommission veröffentlicht eine Liste von Drittländern mit hohem Risiko, die für alle Rechtsträger rechtsverbindlich ist. Darüber hinaus wird von den Unternehmen erwartet, dass sie bei ihrer eigenen internen Risikoeinstufung auch andere Quellen berücksichtigen, z. B. die Listen der Arbeitsgruppe „Bekämpfung der Geldwäsche und der Terrorismusfinanzierung“ (FATF) von „Jurisdiktionen mit hohem Risiko, bei denen Handlungsbedarf geboten ist“ (schwarze Liste) und „Jurisdiktionen unter verstärkter Überwachung“ (graue Liste).

Die Rechtsträger sollten eine interne Liste der Länder mit hohem Risiko erstellen und diese regelmäßig unter Verwendung folgender Quellen aktualisieren:

- EK-Liste der Drittländer mit hohem Risiko
- FATF-Listen (dreimal jährlich aktualisiert)
- Leitlinien der österreichischen Behörden

- Andere renommierte Quellen, darunter Länderberichte von IWF, Weltbank oder Transparency International.

Diese interne Liste muss den entsprechenden Mitarbeitern zugänglich gemacht und während der Sorgfaltspflicht gegenüber Kunden, der Risikoeinstufung und der laufenden Überwachung referenziert werden.

6.2 Konkrete Beispiele

- Ein Immobilienmakler sollte zusätzliche Finanzunterlagen anfordern, wenn ein Käufer Staatsangehöriger eines gelisteten Hochrisikolandes ist oder dort ansässig ist; insbesondere, wenn er ein Unternehmensvehikel oder eine Finanzierung über Dritte nutzt.
- Ein Versicherungsmakler sollte eine strengere Überprüfung vornehmen, wenn ein Antragsteller oder Begünstigter in einem Hochrisikogebiet ansässig sind, einschließlich der Anforderung einer vollständigen Angabe der Herkunft der Mittel.
- Ein Warenhändler sollte ohne vollständige Rückverfolgbarkeit und Begründung keine Barzahlungen oder Transaktionen akzeptieren, die den Weiterverkauf an Hochrisikogebiete beinhalten.
- Ein Unternehmensberater sollte keine Unternehmensstrukturen mit Beteiligung von Anteilseignern oder wirtschaftlichen Eigentümern in Hochrisikoländern ohne eine verstärkte Dokumentation aufbauen.

7 LAUFENDE ÜBERWACHUNG

Sobald eine Geschäftsbeziehung begründet ist, müssen die Unternehmen das Verhalten des Kunden laufend überwachen. Dazu gehört die Überprüfung der Übereinstimmung der Transaktionen mit dem angegebenen Zweck und dem Kundenprofil, die Überprüfung ungewöhnlicher Muster und die Aktualisierung der Sorgfaltspflichten gegenüber Kunden bei allen relevanten Änderungen (z. B. Eigentumsänderung, neue WE oder Länderwechsel).

Sobald eine Geschäftsbeziehung begründet ist, müssen die Unternehmen:

- Die Transaktionen überwachen und mit dem Risikoprofil des Kunden abgleichen
- Die CDD-Daten, insbesondere die WE-Daten und die Risikoeinstufung, auf dem neuesten Stand halten
- Abweichungen von dem erwarteten Verhalten oder unvollständige Antworten untersuchen
- Geeignete Schritte unternehmen, falls zu irgendeinem Zeitpunkt ein Verdachtsmoment entsteht.

Auch wenn Form und Häufigkeit der laufenden Überwachung je nach Sektor unterschiedlich sind, bleibt der Grundsatz unverändert: Überwachung wesentlicher Risikoveränderungen und entsprechendes Handeln. Selbst in transaktionsbasierten Sektoren muss die Überwachung während des gesamten Verpflichtungszeitraums aufrechterhalten werden. Bei



laufenden Geschäftsbeziehungen hat das Unternehmen die Pflicht, wachsam zu bleiben und die Risikoprofile der Kunden zu aktualisieren, sobald neue Informationen verfügbar werden.

8 MELDUNG VERDÄCHTIGER TRANSAKTIONEN

Die Rechtsträger müssen der zentralen Meldestelle (FIU) **unverzüglich** melden, wenn sie wissen oder vermuten, dass eine Transaktion, eine versuchte Transaktion oder Tätigkeit im Zusammenhang mit Geldwäsche oder Terrorismusfinanzierung steht.

Alle Rechtsträger sind rechtlich verpflichtet, verdächtiges Verhalten festzustellen und darauf zu reagieren. Verdächtige Transaktionen können ungewöhnlich große Transaktionen ohne offensichtlichen rechtlichen Zweck sein, eine unerklärliche Beteiligung Dritter beinhalten oder so strukturiert sein, dass gesetzliche Schwellenwerte umgangen werden. Ein Verdacht kann jedoch auch auf Verhaltensweisen wie z. B. die Zurückhaltung eines Kunden bei der Bereitstellung von Informationen, kurzfristige Änderungen bei Begünstigten oder Zahlungen oder auf widersprüchliche Erklärungen zurückzuführen sein.

Sobald ein Verdacht auftritt, selbst wenn die Transaktion noch nicht abgeschlossen ist, darf das Unternehmen die Geschäftsbeziehung nicht ohne vorherige eingehendere Prüfung fortsetzen. Wenn der Verdacht nach dieser Überprüfung fortbesteht und nicht ausgeräumt werden kann, ist der Rechtsträger verpflichtet, über die GoAML-Webplattform bei der zentralen Meldestelle eine Meldung über verdächtige Transaktionen (STR) einzureichen.

Anmeldung:

- Einreichung über das GoAML-Webportal
- Die Berichte sollten Folgendes enthalten:
 - Beteiligte, Transaktionen, Dienstleistungen, Waren und Beträge
 - Beschreibung der verdächtigen Tätigkeit
 - Belege (z. B. Verträge, Zahlungsbelege, Schriftverkehr)
 - Bereits ergriffene Maßnahmen.

Bei einer STR-Meldung müssen die Unternehmen die Verdachtsgrundlage klar beschreiben, alle relevanten Unterlagen vorlegen und die ergriffenen Maßnahmen erläutern. **Wichtig ist, dass die Mitarbeiter ein Tipping-off des Kunden vermeiden; es ist rechtswidrig, einen Kunden darüber zu informieren, dass eine STR eingereicht wurde.**

Zusätzlich dazu sollten Unternehmen ihre internen Aufzeichnungen überprüfen, alle weiteren verdächtigen Tätigkeiten einfrieren (sofern dies gesetzlich zulässig ist) und in Erwägung ziehen, die Geschäftsbeziehung zu beenden, wenn das Missbrauchsrisiko nicht gemindert werden kann.

Kapitel 12 dieses Handbuchs enthält praktische Fälle und Risikoindikatoren, anhand deren die Rechtsträger beurteilen können, ob eine Transaktion möglicherweise einer weiteren Prüfung bedarf, um festzustellen, ob ein begründeter Verdacht besteht, dass die Transaktion oder die Gelder mit einer kriminellen Tätigkeit in Verbindung stehen könnten.



8.1 GoAML-Zugang

Sollte der Verdacht auf Geldwäsche oder Terrorismusfinanzierung bestehen, ist das Unternehmen gesetzlich verpflichtet, der zentralen Meldestelle unverzüglich eine Verdachtsmeldung (STR) zu übermitteln. Solche Berichte können nur über die GoAML-Webplattform eingereicht werden. Selbst wenn die GewO die Rechtsträger nicht ausdrücklich dazu verpflichtet, sich für den Zugang zu GoAML vorab registrieren zu lassen, ist eine unverzügliche Meldung ohne diese in der Praxis nicht möglich. Daher wird den Unternehmen dringend empfohlen, sich **proaktiv bei GoAML anzumelden** und sicherzustellen, dass sie ihren rechtlichen Verpflichtungen unverzüglich nachkommen können, wenn ein Verdachtsfall auftritt.

9 INTERNE MAßNAHMEN ZUR EINHALTUNG DER AML/CFT-VORSCHRIFTEN

Eine starke Governance, klare interne Zuständigkeiten und verhältnismäßige interne Maßnahmen (wie Strategien, Prozesse, Managementsysteme) sind wesentliche Bestandteile der Einhaltung der AML/CFT-Vorschriften, unabhängig von der Größe des Unternehmens. Auch wenn von kleinen Unternehmen nicht erwartet wird, dass sie dieselben Systeme anwenden wie große Unternehmen, müssen auch sie ihre Ernsthaftigkeit und ihr Bewusstsein unter Beweis stellen und ihre Bemühungen zur Verhinderung von Geldwäsche, Terrorismusfinanzierung und Verstößen gegen Sanktionen dokumentieren.

Alle Rechtsträger müssen folgende interne Maßnahmen ergreifen:

- Eine schriftliche risikobasierte AML/CFT-Strategie
- Interne Kontrollverfahren, die in einem angemessenen Verhältnis zu ihrer Größe und ihrer Exposition stehen
- Regelmäßige Schulung der Mitarbeiter
- Ein klares Aufzeichnungssystem.

Diese Anforderungen können in Bezug auf die Größe skaliert werden, müssen jedoch nachweisbar sein.

9.1 Governance

Alle Unternehmen müssen eine klare interne Governance-Struktur einrichten, um sicherzustellen, dass Maßnahmen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung nicht nur formalisiert, sondern auch wirksam umgesetzt werden. Dies bedeutet, dass das Unternehmen die interne Verantwortung für die Überwachung, Anwendung und regelmäßige Überprüfung seiner AML/CFT-Verpflichtungen, unabhängig von seiner Größe, übertragen muss.

Bei kleineren Rechtsträgern, z. B. Einzelunternehmen oder Familienunternehmen, übernimmt der Eigentümer, Geschäftsführer oder Manager typischerweise diese Verantwortung in der Regel direkt. Bei größeren Rechtsträgern mit mehr Mitarbeitern oder Zweigstellen kann die Verantwortung übertragen werden, die letztendliche Rechenschaftspflicht liegt jedoch immer bei der Geschäftsleitung.

Ein Unternehmen kann sich bei der Einhaltung der Vorschriften nicht ausschließlich auf einen externen Steuerberater oder Rechtsanwalt verlassen, es muss auch über internes Bewusstsein und Prozesse verfügen, die auf seine spezifischen Geschäftsrisiken zugeschnitten sind.

9.2 Compliance-Beauftragter oder verantwortliche Person

Jedes Unternehmen muss einen Compliance-Beauftragten oder eine für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung zuständige Person benennen, auch wenn diese Person noch andere Aufgaben innerhalb des Unternehmens innehat. In kleinen und mittleren Unternehmen ist es durchaus akzeptabel, dass der Eigentümer, Geschäftsführer oder die Geschäftsleitung diese Rolle übernehmen. Entscheidend ist, dass die benannte Person über ausreichende Befugnisse, Verständnis und Zeit verfügt, um die Aufgaben wahrzunehmen.

Der Compliance-Beauftragte oder die verantwortliche Person sind zuständig für:

- Gewährleistung der Erfüllung der Sorgfaltspflichten gegenüber Kunden und der fortlaufenden Überwachung
- Überwachung von Risikobewertungen und Aktualisierung der Geschäftsstrategie
- Überprüfung verdächtiger Aktivitäten und Entscheidung über die Einreichung von Verdachtsmeldungen (STR)
- Koordinierung der Zusammenarbeit mit der Aufsichtsbehörde und der zentralen Meldestelle (FIU).

Der Name und die Zuständigkeiten dieser Person sollten in internen Strategiedokumenten dokumentiert und bei Aufsichtsinspektionen zur Verfügung gestellt werden.

9.3 Internes Audit oder unabhängige Überprüfung (proportional zur Größe)

Bei größeren Unternehmen, insbesondere solchen mit mehreren Filialen, Servicelinien oder kundenorientierten Mitarbeitern, ist ein unabhängiges Audit oder ein interner Überprüfungsmechanismus erforderlich. Dies bedeutet nicht unbedingt die Einstellung eines externen Prüfers, sondern vielmehr die Sicherstellung, dass die AML/CFT-Verfahren regelmäßig von einer Person überprüft werden, die nicht unmittelbar an den täglichen Compliance-Maßnahmen beteiligt ist.

Bei kleinen Unternehmen kann eine jährliche Selbstkontrolle oder Peer Review (z. B. durch einen anderen Geschäftsführer oder Geschäftspartner) ausreichen, sofern sie dokumentiert ist. Unternehmen sollten die Angemessenheit ihrer Risikobewertungen, die Qualität der Due-Diligence-Dossiers und die Aktualität der Verdachtsmeldungen (STR) bewerten. Etwaige Schwachstellen oder Lücken sollten korrigiert werden.

9.4 Schulung und Sensibilisierung

Alle Personen, die an CDD, Transaktionsabwicklung oder Management beteiligt sind (einschließlich Zeitbedienstete oder Freiberufler), müssen regelmäßige AML/CFT-Schulungen erhalten. Der Inhalt der Schulung sollte in einem angemessenen Verhältnis zu ihren Zuständigkeiten stehen und die spezifischen Risiken widerspiegeln, denen Unternehmen und Sektor ausgesetzt sind.

In kleinen Unternehmen kann dies wie folgt aussehen:



- Interne Sitzungen unter der Leitung des Compliance-Beauftragten oder der verantwortlichen Person.
- Online-Schulungsmodule (z. B. über Wirtschaftskammern oder Branchengremien).
- Dokumentierte Überprüfungen neuer AML/CFT-Typologien und Warnsignale.

Die Schulung muss mindestens alle zwei Jahre und bei Änderung der einschlägigen Rechtsvorschriften oder internen Strategien durchgeführt werden. Es sind Schulungsunterlagen zu führen, die die Namen der Teilnehmer, das Datum und die behandelten Themen enthalten.

9.5 Negative Berichte

Die Aufsichtsbehörde kann Unternehmen auffordern zu bestätigen, ob sie in den Geltungsbereich der AML/CFT-Verpflichtungen nach der GewO fallen. In Fällen, in denen ein Unternehmen diesen Verpflichtungen nicht unterliegt, wird nachdrücklich empfohlen, eine negative Bestätigung („negativer Bericht“) vorzulegen, woraus dies hervorgeht. Auch wenn derzeit keine ausdrückliche rechtliche Verpflichtung zur Vorlage eines solchen Berichts besteht, führt das Versäumnis darauf zu reagieren, zu Unsicherheit darüber, ob das Unternehmen davon befreit ist oder lediglich gegen die Vorschriften verstößt. In solchen Fällen kann eine Vor-Ort-Inspektion erforderlich sein, um die Situation zu klären. Die proaktive Vorlage eines negativen Berichts trägt dazu bei, unnötigen Verwaltungsaufwand sowohl für das Unternehmen als auch für die Aufsichtsbehörden zu vermeiden, und gilt als bewährtes Verfahren im Einklang mit risikobasierten Aufsichtsgrundsätzen.

10 AUFBEWAHRUNG VON AUFZEICHNUNGEN

Die Rechtsträger müssen alle einschlägigen AML/CFT-Dokumente mindestens fünf Jahre lang aufbewahren, es sei denn, eine längere Aufbewahrung ist aus rechtlichen oder regulatorischen Gründen erforderlich.

Dies umfasst:

- CDD-Informationen und Dokumente zur Identifizierung (z. B. ID-Kopien, WE-Dokumentation)
- Risikobewertungen
- Transaktionsaufzeichnungen (z. B. Rechnungen, Verträge, Zahlungsunterlagen)
- Vermerke, E-Mail-Mitteilungen und Erläuterungen zu STR-Entscheidungen
- Eingereichte STR und zugehörige Unterlagen.

Die Aufzeichnungen müssen so aufbewahrt werden, dass sie auf Ersuchen der Aufsichtsbehörde oder der zentralen Meldestelle schnell abgerufen werden können. Sowohl elektronische als auch physische Formate sind zulässig, sofern sie sicher und fälschungssicher sind.

Die Verpflichteten müssen bei Inspektionen oder Dokumentenanfragen uneingeschränkt mit den Aufsichtsbehörden zusammenarbeiten und nachweisen können, dass sie CDD und Risikobewertungen durchführen, das Personal schulen und verdächtige Tätigkeiten melden.



11 SEKTORSPEZIFISCHE LEITLINIEN

Die nachstehenden Fallstudien stützen sich auf realistische Typologien, von denen viele auf tatsächlichen Fällen oder international bewährten Verfahren beruhen. Sie sollen kein Fehlverhalten der Sektoren selbst implizieren, sondern als pädagogische Instrumente für die Risikominderung und die interne Schulung dienen.

Die Risikoindikatoren sind in fünf Kategorien gegliedert:

- Kundeneigenschaften
- Geografische Exposition
- Lieferkanäle
- Transaktionen
- Dienstleistungen oder Produkte

Jede Untergruppe ist auf die spezifischen Dienstleistungen, Produkttypen und Kundenprofile zugeschnitten, die für einen Sektor relevant sind.

Rechtsträger können diese praktischen Fälle und Risikoindikatoren heranziehen, um zu beurteilen, ob eine Transaktion einer weiteren Prüfung bedarf, damit festgestellt werden kann, ob der begründete Verdacht besteht, dass die Transaktion oder die Gelder mit einer kriminellen Tätigkeit in Verbindung stehen könnten, die dann unverzüglich der zentralen Meldestelle gemeldet werden sollte.

11.1 Immobilienmakler

Bei Immobilienmaklern beginnt der risikosensitive Ansatz mit der Feststellung, dass nicht alle Transaktionen das gleiche Risikoniveau aufweisen. Ein Erstkäufer, der im eigenen Namen eine bescheidene Wohnung erwirbt und über eine österreichische Bank finanziert, stellt ein minimales AML/CFT-Risiko dar. In solchen Fällen können standardisierte CDD-Maßnahmen (Überprüfung der Identität, Bestätigung der Finanzierung durch eine Bank und Dokumentation des Kundenrisikoprofils) ausreichen.

Dagegen stellt der Verkauf einer hochwertigen Immobilie an einen ausländischen Käufer, der eine komplexe Struktur nutzt oder zur Finanzierung einen unabhängigen Dritten beauftragt, ein deutlich höheres Risiko dar. In diesen Fällen sollte der Makler die EDD anwenden, z. B. indem er den WE überprüft, Unterlagen über die Herkunft der Mittel verlangt und Open-Source-Nachforschungen zu allen Beteiligten durchführt.

Ein risikosensitiver Ansatz bedeutet auch, auf bestimmte Warnsignale zu achten, wie z. B. Druck zur Vermeidung einer formalen Finanzierung, Zurückhaltung bei der Offenlegung des Zwecks der Immobilie oder Bemühungen, Zahlungen zu stückeln, um Meldeschwellen zu vermeiden. In solchen Fällen sollte der Makler den Fall intern eskalieren, alle Entscheidungen dokumentieren und, falls Verdachtsmomente bestehen bleiben, eine Verdachtsmeldung (STR) einreichen.

Im Immobiliensektor sind Kundenbeziehungen oft transaktionsbasiert und von kurzer Dauer. Die laufende Überwachung bleibt jedoch während der Dauer einer Immobilientransaktion von der Unterzeichnung des Mandats bis zum Abschluss des Verkaufs relevant.

Immobilienmakler sollten auf Änderungen bei der Mittelherkunft, der Finanzierungsstruktur oder der Eigentümerschaft achten, insbesondere wenn solche Änderungen erst spät im

Prozess oder ohne Begründung vorgenommen werden. Wenn ein Käufer zunächst beabsichtigt, eine Hypothek in Anspruch zu nehmen, später aber eine ungeklärte Banküberweisung oder Barzahlung durch Dritte vornimmt, muss der Makler das Risiko neu bewerten und erforderlichenfalls eine zusätzliche Überprüfung vornehmen oder einen Verdacht melden. Auch wenn die Geschäftsbeziehung möglicherweise nicht langfristig angelegt ist, ist eine kontinuierliche Sensibilisierung während der gesamten Transaktion erforderlich.

11.1.1 Fallstudien und Warnsignale

Immobilienmakler müssen sektorspezifische Warnsignale bewerten und erkennen. Im folgenden Abschnitt werden Fallstudien zur Bekämpfung von Geldwäsche, Terrorismusfinanzierung und Sanktionen sowie Risikoindikatoren aus verschiedenen Quellen zusammengefasst.

Fallstudie 1: Nutzung von hochwertigen Immobilien zum Verschleiern illegaler Erträge (Layering)

Eine PEP aus einem Drittland erwarb eine hochwertige Wohnung in Wien über eine komplexe Struktur, an der mehrere in verschiedenen Jurisdiktionen eingetragene Unternehmen beteiligt waren. Die Geldmittel wurden über Konten in Zypern und den Vereinigten Arabischen Emiraten nach Österreich geschleust. Die Immobilie stand leer.

Warnsignale:

- Komplexe Eigentumskette
- Nutzung ausländischer Unternehmen
- Keine erklärte wirtschaftliche Tätigkeit oder Einkünfte im Zusammenhang mit dem Kauf
- Leerstehende Immobilie.

Fallstudie 2: Terrorismusfinanzierung durch gewerbliche Vermietung

Eine Gruppe, die mit einem bekannten terroristischen Netzwerk in Verbindung stand, mietete eine Gewerbefläche über einen Strohmann an. Der Rechtsträger, auf den der Mietvertrag lief, war unter einem anderen Namen eingetragen und erschien legitim. Es wurden regelmäßig Geldmittel von mehreren Konten überwiesen, immer knapp unterhalb der Meldeschwelle. Diese Zahlungen wurden später mit der logistischen Unterstützung extremistischer Operationen im Ausland in Verbindung gebracht.

Warnsignale:

- Unerklärliche häufige kleine Zahlungen
- Diskrepanz zwischen der angegebenen Geschäftstätigkeit und der tatsächlichen Nutzung der Immobilie
- Beteiligung von Stroh Männern
- Anmietung durch einen neu eingetragenen Rechtsträger ohne Vorgeschichte.



Fallstudie 3: Versuchter indirekter Immobilienerwerb eines mit Sanktionen belegten Unternehmens

Ein von Russland kontrolliertes Unternehmen, deren indirekter Eigentümer eine mit Sanktionen belegte Person ist, versuchte, über eine luxemburgische Holdingstruktur in Salzburg Immobilien zu erwerben. Eine örtliche Immobilienagentur vermittelte das Geschäft in Unkenntnis des WE. Die Transaktion wurde während des notariellen Verfahrens gemeldet und von den Behörden blockiert.

Warnsignale:

- Verwendung komplexer Rechtsstrukturen, um die Eigentümerschaft zu verschleiern
- WE, der in Verbindung mit sanktionierten Jurisdiktionen steht
- Immobilienmakler identifizierte den tatsächlichen WE nicht ordnungsgemäß
- Versuchte Umgehung von EU-Sanktionen.

Fallstudie 4: Integration mithilfe von Renovierungsprojekten

Kriminelle Erträge aus Mehrwertsteuerbetrug wurden durch wiederholte Ankäufe und Renovierungen älterer Immobilien in Vorstädten gewaschen. Die Renovierungskosten wurden mithilfe gefälschter Rechnungen, die von Mantelgesellschaften ausgestellt wurden, aufgeblasen. Die Immobilien wurden dann zu überhöhten Preisen an verbundene Unternehmen verkauft.

Warnsignale:

- Wiederholte Transaktionen innerhalb kurzer Zeiträume
- Hohe Renovierungskosten ohne klare Begründung
- Nutzung von Offshore-Bauunternehmen
- Schneller Weiterverkauf an verbundene Parteien.

Fallstudie 5: Bargeldankauf ländlicher Flächen

Ein Käufer aus einem Hochrisikogebiet erwarb mehrere landwirtschaftliche Grundstücke in bar zu „Investitionszwecken“. Das Land wurde nicht erschlossen und ein Teil der Grundstücke wurde erneut innerhalb desselben Netzes weiter übertragen. Das Profil und das Einkommensniveau des Käufers entsprachen nicht dem Transaktionsvolumen.

Warnsignale:

- Bargeldankäufe ohne Finanzierung
- Nicht genutzte oder erschlossene Flächen
- Käufer aus einem Hochrisikoland
- Diskrepanz zwischen Einkommensprofil und Transaktionsvolumen.

Fallstudie 6: Verdeckte Eigentümerschaft durch komplexe Strukturen

Eine Immobilienagentur vermittelte den Verkauf einer hochwertigen Wohnimmobilie in einer Großstadt. Bei dem Käufer handelte es sich um ein Unternehmen, das in einer Offshore-Jurisdiktion mit einem nicht namentlich benannten WE registriert war. Das Unternehmen wurde über einen Intermediär eingeführt, der die Kommunikation übernahm. Die



Immobilienfirma führte weder eine unabhängige Überprüfung der Identität des WE durch, noch erkundigte sie sich nach der Mittelherkunft. Die Immobilie stand mehrere Jahre lang leer.

Warnsignale:

- Transaktionen mit undurchsichtigen Strukturen ohne klare wirtschaftliche Begründung
- Nicht benannter oder nicht offengelegter WE
- Verlass auf Intermediäre ohne angemessene Sorgfaltsprüfung
- Leerstehende Immobilie nach dem Verkauf.

Fallstudie 7: Komplexe Finanzstrukturen und Sanktionsexposition

Eine Luxusimmobilie in einer bekannten Ferienregion wurde von einem ausländisch kontrollierten Unternehmen mit Verbindungen zu mehreren Offshore-Unternehmen erworben. Die Finanzierung stammte aus Jurisdiktionen, die für das Bankgeheimnis bekannt sind. Der Käufer wurde von einer Anwaltskanzlei vertreten, die es unter Berufung auf die Vertraulichkeitspflicht ablehnte, detaillierte Informationen über die Eigentumsverhältnisse bereitzustellen. Der an dem Verkauf beteiligte Immobilienmakler stellte angesichts der rechtlichen Vertretung und der vollständigen Vorauszahlung keine weiteren Fragen.

Warnsignale:

- Eigentümerschaft verbunden mit mehrschichtigen Offshore-Firmen
- Mangelnde Transparenz in Bezug auf die wirtschaftlichen Eigentümer
- Finanzierung aus Jurisdiktionen, die dem Bankgeheimnis unterliegen
- Rechtsvertreter verweigerte die Offenlegung von Eigentumsangaben unter Berufung auf die Vertraulichkeit
- Immobilienmakler akzeptierte diese Erklärung ohne weitere Nachforschungen
- Vollständige Vorauszahlung akzeptiert, ohne Überprüfung der Mittelherkunft.

Fallstudie 8: Unklare Mittelherkunft bei Transaktionen zwischen verbundenen Unternehmen und Personen

Eine Immobilie wurde zwischen zwei Personen, die zuvor in einer persönlichen Beziehung zueinanderstanden, für 750.000 EUR verkauft. Die Zahlung erfolgte über einen Notar und wurde über ein Geschäftskonto abgewickelt. Kurz vor der Transaktion ging auf diesem Konto eine große Bareinlage ein, und kurz danach wurde ein erheblicher Teil der Gelder in bar an den Käufer zurückgegeben, um angeblich eine informelle Schuld zu begleichen. Die Personen machten geltend, dass das Geld aus privaten Ersparnissen im informellen Sektor (z. B. Gebrauchtwagenhandel) stamme und aus steuerlichen Gründen nicht angemeldet wurde. Es lagen keine Unterlagen vor, die die Herkunft der Mittel oder die geltend gemachte Schuldenregelung belegten.

Warnsignale:

- Transaktion zwischen Privatpersonen mit enger persönlicher Beziehung
- Zahlung über ein Geschäftskonto, nicht über ein persönliches Konto
- Große Bareinlage auf dem Konto kurz vor der Transaktion
- Nach dem Verkauf abgehobene und an den Käufer zurückgegebene Barmittel

- Herkunft der Mittel aus nicht angemeldeten privaten Ersparnissen im informellen Sektor.

Fallstudie 9: Ungewöhnliche ausländische Finanzierungsvereinbarung

Eine 30-jährige österreichische Staatsbürgerin veranlasste den Erwerb einer Wohnimmobilie in Salzburg in Höhe von 900.000 EUR. Obgleich sie offiziell als einzige Käuferin aufgeführt wurde, wurden alle Vertrags- und Finanzverhandlungen von ihrem Partner geführt. Die angemeldete Finanzierung erfolgte in Form eines „Darlehens“ eines privaten Unternehmens mit Sitz in einem Hochrisikogebiet. Es wurde weder ein Rückzahlungsplan noch ein Bankkonto für die Rückzahlung angegeben. Von mehreren Drittfirmen im Ausland wurden mehrere gestaffelte Zahlungen geleistet, was Fragen nach der tatsächlichen Herkunft der Mittel aufwarf.

Warnsignale:

- Eigentum und Kontrolle des Erwerbs aufgeteilt zwischen dem offiziellen Käufer und dem tatsächlich Handelnden
- Ausländische Finanzierung ohne eindeutige Rückzahlungsverpflichtungen
- Nutzung mehrerer unabhängiger Unternehmen für Geldtransfers
- Hohes Darlehen, das in keinem Verhältnis zum Finanzprofil des Käufers steht.

11.1.2 Risikoindikatoren für Immobilienmakler

1. Indikatoren für das Kundenrisiko

- Kunde ist eine PEP, insbesondere aus Drittländern mit hohem Risiko
- Beteiligung von Strohmännern oder Vertretern mit begrenzter Kenntnis der Transaktion
- Kunde ist ungewöhnlich zögerlich, Informationen über den WE oder die Mittelherkunft bereitzustellen.
- Diskrepanz zwischen dem Profil des Kunden (z. B. Studenten, Arbeitslose) und dem Transaktionswert
- Transaktionen mit Kunden aus Ländern mit aktiven EU-Sanktionen oder TF-Bedenken
- Kunden, die komplexe juristische Personen oder Trusts ohne klaren Geschäftszweck nutzen
- Zurückhaltung oder Ablehnung der Offenlegung von WE oder der Vorlage von Ausweisdokumenten
- Kunden aus Jurisdiktionen mit hohem Korruptionsniveau oder unter internationalen Sanktionen
- Diskrepanz zwischen dem bekannten Einkommen des Kunden und dem Wert der Immobilientransaktion.

2. Geografische Risikoindikatoren

- Immobilien in Grenzgebieten, Skiregionen oder tourismusintensiven Gebieten mit einem hohen Anteil gebietsfremder Käufer



- Transaktionen mit Kunden oder Finanzierung aus Hochrisikogebieten oder nicht kooperativen Jurisdiktionen
- Käufer, die mit Gebieten mit bekannten Terrorismusfinanzierungsnetzen in Verbindung stehen
- Immobilien in Regionen mit hoher Nachfrage durch ausländische Investoren wie Skigebiete oder Großstädte
- Transaktionen mit Geldern aus Ländern, bei denen ein hohes Risiko der Geldwäsche oder Terrorismusfinanzierung festgestellt wurde
- Beteiligung von Offshore-Finanzzentren, die für Geheimhaltung und mangelnde Transparenz bekannt sind.

3. Risikoindikatoren der Lieferkanäle

- Einsatz von Vermittlern (Rechtsanwälte, Notare, Makler) ohne physische Interaktion mit dem Endkunden
- Nutzung von Remote Onboarding und elektronischer Dokumentation ohne weitere Überprüfung
- Übermäßiges Vertrauen auf professionellen Zusicherungen (z. B. „von einem Drittunternehmen überprüft“ ohne eigene Kontrolle)
- Transaktionen, die vollständig online oder über Vermittler ohne persönliche Treffen durchgeführt werden
- Rückgriff auf Dritte, z. B. Rechtsanwälte oder Makler, um die Identität des Kunden zu verschleiern
- Rasche Abfolge von Immobilienankäufen und -verkäufen ohne klare wirtschaftliche Begründung.

4. Risikoindikatoren bei Transaktionen

- Bargeldintensive Transaktionen, insbesondere über 10.000 EUR
- Über- oder unterbewertete Immobilien ohne Marktbegründung
- Back-to-Back-Transaktionen (Immobilien werden nach dem Erwerb rasch weiterverkauft)
- Nutzung von Kryptowährungen oder alternativen Finanzierungsstrukturen
- Beteiligung mehrerer Länder an der Finanzierung des Geschäfts
- Zahlungen in bar oder über komplexe Finanzinstrumente
- Über- oder Unterbewertung von Immobilien im Vergleich zum Marktpreis
- Verwendung von Darlehen oder Hypotheken von nicht traditionellen Kreditgebern ohne klare Bedingungen
- Sofortiger Weiterverkauf von Immobilien zu erheblich unterschiedlichen Preisen.

5. Risikoindikatoren für Dienstleistungen/Immobilien

- Erwerb von Immobilien, die lange Zeit leer stehen oder nicht erschlossen werden
- Nutzung von land- oder forstwirtschaftlichen Flächen als Front für Wertspeicherung
- Anmietung von Immobilien für unklare oder falsch dargestellte Geschäftstätigkeiten
- Lange Zeit leerstehende oder unerschlossene Immobilien

- Häufige Renovierungen oder Änderungen der Immobiliennutzung ohne klare Begründung
- Mietvereinbarungen mit Mietern, die über dem Markt liegende Mieten ohne eindeutige Einkommensquelle zahlen
- Immobilien, die für Zwecke verwendet werden, die nicht mit den Bauordnungsbestimmungen oder der erklärten Verwendung vereinbar sind.

11.2 Versicherungsvermittler

Versicherungsvermittler sollten je nach Art des Produkts und der Transaktion zwischen Kunden mit geringem und hohem Risiko unterscheiden. So stellt beispielsweise ein junger Österreicher, der eine Basisversicherung abschließt, ein geringes Risiko dar und daher ist nur eine Standard-CDD-Prüfung erforderlich.

Dagegen sollte ein Kunde, der eine Lebensversicherung mit hoher Einmalprämie abschließt, insbesondere, wenn sie von einem Dritten bezahlt wird, sorgfältiger überprüft werden. In einem solchen Fall sollte sich der Vermittler nach der wirtschaftlichen Begründung der Versicherungspolice, der Mittelherkunft sowie der Berufs-, Einkommens- oder Vermögenssituation des Kunden erkundigen. Außerdem sollte bei einem Kunden, der die Versicherungspolizze innerhalb kurzer Zeit storniert oder den Begünstigten auf einen Nicht-Familienangehörigen umändert, eine verstärkte Überprüfung durchgeführt werden.

Ein risikosensitiver Ansatz bedeutet auch, dass indirekte Risikoindikatoren wie Ansässigkeit im Ausland, die Nutzung ausländischer Unternehmen für Prämienzahlungen oder komplexe vertragliche Vereinbarungen berücksichtigt werden müssen. In solchen Fällen können verstärkte Kontrollen und möglicherweise Berichtspflichten erforderlich sein.

Für Versicherungsvermittler ist eine kontinuierliche Überwachung von wesentlicher Bedeutung, insbesondere bei Lebensversicherungen oder Anlagenprodukten, die jahrelang aktiv bleiben können. Zu den Überwachungspflichten zählen die Gewährleistung, dass Prämienzahlungen dem Kundenprofil entsprechen, die Erkennung verdächtiger Änderungen der Versicherungspolice (z. B. plötzliche Änderung des Begünstigten oder vorzeitige Auszahlung) sowie die Neuvalidierung der Kundeninformationen, wenn sich die Umstände des Kunden ändern. Wenn ein Kunde, der eine Police erst vor einigen Jahren abgeschlossen hat, nun eine vollständige Barauszahlung auf ein Auslandskonto fordert, muss der Vermittler prüfen, ob dieses Verhalten mit dem ursprünglichen Risikoprofil im Einklang steht. Regelmäßige Überprüfungen sollten risikobasiert sein: Risikoreichere Kunden oder Polizzen sollten häufiger oder bei bestimmten Auslösern (z. B. Anträge auf Änderung der Polizze) überprüft werden.

11.2.1 Fallstudien und Warnsignale

Versicherungsvermittler müssen sektorspezifische Warnsignale bewerten und erkennen. Im folgenden Abschnitt werden allgemeine Fallstudien zu Geldwäsche, Terrorismusfinanzierung und Sanktionen sowie Risikoindikatoren aus verschiedenen Quellen zusammengefasst.

Fallstudie 1: Lebensversicherungspolizze zur Verschleierung von Erträgen aus Straftaten

Ein Vermittler vermittelte den Verkauf einer Lebensversicherung mit einer Einmalprämie von 250.000 EUR an einen Kunden mit begrenztem Einkommen. Die Polizze erlaubte eine vorzeitige Auszahlung bei minimaler Strafe. Die Police wurde nur sechs Monate später gekündigt, und die Mittel wurden auf ein Konto auf einen anderen Namen in einem anderen EU-Mitgliedstaat überwiesen.

Warnsignale:

- Hohe Einmalprämie, die nicht dem Einkommen entspricht
- Vorzeitige Kündigung kurz nach Abschluss
- Grenzüberschreitende Geldtransfers an Dritte.

Fallstudie 2: Terrorismusfinanzierung durch Versicherungsauszahlung

Eine Versicherungspolice wurde unter Verwendung einer falschen Identität für eine Gruppe von Personen erworben, die in ein Konfliktgebiet reisten. Nach dem Tod eines Mitglieds wurde die Versicherung auf ein Bankkonto ausgezahlt, das von einem Dritten kontrolliert wurde, gegen den wegen Terrorismusfinanzierung ermittelt wurde. Der Vermittler überprüfte die Original-Ausweisdokumente nicht.

Warnsignale:

- Kurz vor einer Reise in Hochrisikoregionen abgeschlossene Versicherungspolicen
- Zahlung an nicht verbundene Dritte
- Verwendung gefälschter Dokumente oder Identitätskonflikte.

Fallstudie 3: Nutzung einer Rentenversicherung durch eine sanktionierte Person

Ein Vermittler verkaufte ein Rentenversicherungsprodukt in Höhe von 400 000 EUR an eine Kapitalgesellschaft. Der WE des Unternehmens war eine mit Sanktionen belegte russische Person. Die Zahlungen liefen über eine zyprische Bank, und in der Polizza wurde ein Familienmitglied als Begünstigter genannt. Der Vermittler hat den WE nicht identifiziert.

Warnsignale:

- Verwendung undurchsichtiger Unternehmensvehikel
- Zahlung über Offshore-Banken
- Verbindung zu sanktionierten Personen/Familien.

Fallstudie 4: Überfinanzierte Lebensversicherungspolice zur Vermögensübertragung

Ein Vermittler half beim Abschluss einer allgemeinen Lebensversicherungspolice mit Überfinanzierung in Höhe von insgesamt 1,2 Mio. EUR über einen Zeitraum von zwei Jahren. Der Kunde war eine PEP außerhalb der EU. Die Polizza wurde später auf eine Offshore-Trust-Struktur übertragen, was die Rückverfolgung der Vermögenswerte erschwerte.

Warnsignale:

- Erhebliche Überfinanzierung ohne klare wirtschaftliche Begründung
- Eigentumsübertragung der Polizza auf Offshore-Trusts
- Beteiligung einer PEP.

Fallstudie 5: Prämien unabhängiger Offshore-Unternehmen

Ein Vermittler akzeptierte wiederkehrende Zahlungen für ein Versicherungsprodukt eines Offshore-Unternehmens aus der Karibik, während der Versicherungsnehmer ein in Österreich wohnhafter Rentner ohne bekannte Geschäftsbeziehungen war. Auf Nachfrage machte der Kunde geltend, dass es sich um „Familienunterstützung“ handele.

Warnsignale:

- Prämien, die von Dritten ohne klare Beziehung gezahlt werden
- Offshore-Finanzierungsquelle entspricht nicht dem Kundenprofil



- Vage oder nicht überprüfbare Erläuterung der Zahlungsquelle.

Fallstudie 6: Schneller Kauf und Kündigung der Police

Mehrere Kunden, die von ein und demselben Intermediär vermittelt wurden, kauften Lebensversicherungspolicen mit kurzer Laufzeit, die vollständig über Guthabekarten bezahlt wurden. Diese wurden innerhalb weniger Wochen gekündigt, wobei Erstattungen auf Konten in Drittländern beantragt wurden. Bei mehreren Kunden zeigte sich ein koordiniertes Verhaltensmuster.

Warnsignale:

- Mehrfache Abschlüsse kurzfristige Versicherungspolicen und deren Kündigung
- Zahlungen über nicht traditionelle Instrumente (z. B. Guthabekarten)
- Erstattungen auf ausländische Konten außerhalb des Zuständigkeitsbereichs des Kunden.

Fallstudie 7: Schneller Ausstieg aus der Lebensversicherungspolice

Ein Kunde kaufte eine Lebensversicherungspolizze mit einer einmaligen Prämienzahlung von 25.000 EUR. Innerhalb weniger Monate kündigte der Kunde die Polizze und verlangte die Auszahlung auf ein anderes als das ursprüngliche Konto. Der Kunde hatte keine Versicherungsvorgeschichte und konnte die Herkunft der Gelder nicht belegen. Open-Source-Nachforschungen ergaben Verbindungen zu einem Unternehmen, das an internationalem Betrug beteiligt ist.

Warnsignale:

- Hohe einmalige Prämienzahlung.
- Rascher vorzeitiger Ausstieg aus der Police.
- Erstattungsantrag auf ein anderes Konto.
- Keine Versicherungsvorgeschichte oder plausibler Versicherungsbedarf.
- Kunde wird mit Betrug in Verbindung gebracht.

11.2.2 Risikoindikatoren für Versicherungsvermittler

1. Indikatoren für das Kundenrisiko

- Kunde ist eine PEP oder eng mit einer solchen verbunden
- Kunde hat keinen eindeutigen Versicherungsbedarf (z. B. wenn ältere Kunden Kinderschutzversicherungen erwerben)
- Häufiger Wechsel zwischen Produkten oder Anbietern
- Verweigerung von Vermögens-/Fonstdokumenten
- Rückgriff auf Dritte als Antragsteller oder Zahler.

2. Geografische Risikoindikatoren

- Kunden oder Prämienzahlungen stehen in Verbindung mit Drittländern mit hohem Risiko (z. B. mit Sanktionen belegte Jurisdiktionen)
- Häufige Reisen oder Aktivitäten des Versicherungsnehmers in Konfliktgebiete oder TF-Hotspots

- Begünstigte sind in Hochrisikogebieten oder nicht kooperativen Jurisdiktionen ansässig.

3. Risikoindikatoren der Lieferkanäle

- Remote Onboarding ohne physische Treffen oder Video-Überprüfung
- Policen werden über nicht reglementierte Makler oder sog. Introducer verkauft
- Nutzung rein digitaler Kommunikationswege bei hohen Policen.

4. Risikoindikatoren bei Transaktionen

- Hohe einmalige Prämienzahlungen, die nicht mit dem Profil übereinstimmen
- Vorzeitiger Ausstieg oder Kündigung mit Auszahlung auf ein nicht verbundenes Konto
- Zahlungen von Offshore-Bankkonten oder Nichtkundenkonten
- Verwendung von Krypto- oder Prepaid-Instrumenten zur Finanzierung von Prämien.

5. Risikoindikatoren für Dienstleistungen/Produkte

- Flexible oder übertragbare Produkte, die als kurzfristige Wertspeicherung verwendet werden
- Ungewöhnliche Versicherungskombinationen (z. B. gebündelte Investitionen plus hohe Lebensversicherung ohne abhängige Personen)
- Wiederholter Ankauf und schnelle Kündigung von Policen
- Nutzung von Versicherungspolicen zur Kanalisierung von Erbschaften oder Vermögensübertragungen
- Hohe Einmalprämienversicherungen ohne logischen Versicherungsbedarf.

11.3 Händler

Händler, die mit Waren wie Autos, Uhren, Kunst, Gold und Schmuck handeln, müssen das Risiko differenzierter einschätzen. Ein Wiederholungskunde, der einen einzelnen hochwertigen Gegenstand mittels einer rückverfolgbaren Banküberweisung über ein inländisches Konto erwirbt, kann als risikoarm eingestuft werden, insbesondere wenn der Kauf seinem Profil entspricht. Dagegen sollte ein Einmalkäufer, der Barzahlung anbietet, keine Rechnung verlangt oder mehrere Personen am Zahlungsprozess beteiligt, als hohes Risiko angesehen werden.

Der Händler sollte den Ausweis verlangen, Fragen zum Hintergrund und zur Beschäftigung des Käufers stellen und in Fällen, in denen die Zahlungen gestückelt oder über Dritte abgewickelt werden, die Einreichung einer STR in Erwägung ziehen.

Ein risikosensitiver Ansatz bedeutet auch, zwischen dem Verhalten von Kleinanlegern und professionellen Wiederverkäufern zu unterscheiden, die im Namen verdeckter Parteien handeln können. Besondere Vorsicht sollte bei Kunden gelten, die an dem Produkt selbst uninteressiert zu sein scheinen, versuchen, Dokumentation zu vermeiden oder auf einer raschen Lieferung in Drittländer bestehen.

Händler haben häufig mit Einzeltransaktionen zu tun. In solchen Fällen ist eine laufende offizielle Überwachung in der Regel nicht erforderlich. Wenn ein Kunde jedoch im Laufe der Zeit mehrere Transaktionen oder umfangreiche Käufe tätigt, sollte der Händler ein kumulatives Profil der Kundentätigkeit aufbewahren. Treten Muster auf, wie häufige hochwertige Ankäufe, die über unabhängige Dritte bezahlt werden, oder wiederholte Ausfuhrersuchen in Länder mit hohem Risiko, sollte der Händler die Risikoeinstufung des Kunden neu bewerten und möglicherweise eine STR einreichen. Händler sollten auch auf verbundene Kunden oder Intermediäre achten, insbesondere wenn dieselben Personen wiederholt bei Transaktionen in Erscheinung, an denen verschiedene Käufer beteiligt sind.

11.3.1 Fallstudien und Warnsignale

Händler müssen sektorspezifische Warnsignale bewerten und erkennen. Im folgenden Abschnitt werden gemeinsame Fallstudien zu Geldwäsche, Terrorismusfinanzierung und Sanktionen sowie Risikoindikatoren aus verschiedenen Quellen zusammengefasst.

Fallstudie 1: Bargeldkäufe von Luxusfahrzeugen ohne wirtschaftliche Begründung

Ein Autohändler akzeptierte mehrere Barzahlungen einer Person, die über mehrere Monate Fahrzeuge der Luxus-Klasse kaufte. Der Käufer hatte kein sichtbares Einkommen und behauptete, ein kleines Import-Export Unternehmen zu betreiben. Die Fahrzeuge wurden kurz zugelassen und anschließend in ein Drittland außerhalb der EU ausgeführt. Der Händler hatte keine EDD durchgeführt.

Warnsignale:

- Bartransaktionen über 10.000 EUR
- Ausfuhr in Jurisdiktionen mit hohem Risiko
- Kundenprofil nicht mit der Kaufskala vereinbar
- Fehlende Finanzierung oder Leasing.

Fallstudie 2: Erwerb von Schmuck durch ein mit Sanktionen belegtes Unternehmen

Ein Luxusjuwelier verkaufte mehrere hochwertige Schmuckstücke an einen Kunden, der mit einer Unternehmenskarte bezahlte, die mit einem Unternehmen verbunden war, das unter der Kontrolle einer mit Sanktionen belegten russischen Person steht. Der Käufer vermied die Offenlegung der WE und führte an, es handele sich bei dem Schmuck um „Unternehmensgeschenke“. Der Juwelier führte weder ein Screening auf Sanktionen durch, noch forderte er Unterlagen über die Eigentumsverhältnisse des Unternehmens an.

Warnsignale:

- Nutzung von juristischen Personen mit undurchsichtigen Eigentumsverhältnissen
- Hochwertige Waren werden als „Geschenke“ erworben
- Keine Klarheit über die Endverwendung oder den Empfänger
- Verbindungen zu Personen, gegen die Sanktionen verhängt wurden.

Fallstudie 3: Nutzung von Kunst zur Geldwäsche

Ein Händler zeitgenössischer Kunst verkaufte wiederholt Werke an denselben ausländischen Käufer, wobei die Preise innerhalb kurzer Zeit unverhältnismäßig stark anstiegen. Die Zahlung erfolgte über verschiedene Intermediäre. Der Käufer bat um eine Lagerung in Österreich und nahm die Kunstwerke nicht physisch in Besitz. Später wurden dieselben Werke über eine Partnergalerie „zurückgekauft“.

Warnsignale:

- Künstliche Preisinflation
- Keine Lieferung oder Nutzung der erworbenen Waren
- Zirkuläre Transaktionen mit verbundenen Unternehmen
- Anonyme Käufer, die Vermittler einsetzen.

Fallstudie 4: Terrorismusfinanzierung über Gold und Edelmetalle

Ein Goldhändler vermittelte einem Unternehmen, das später mit Terrorismusfinanzierung in Verbindung gebracht wurde, mehrere Transaktionen. Das Unternehmen kaufte große Mengen Altgold an und bezahlte in mehreren kleinen Banküberweisungen aus Konten in der gesamten EU. Ein Teil des Goldes wurde eingeschmolzen und in die Türkei verbracht. Die CDD beschränkte sich auf Dokumente aus dem Unternehmensregister.

Warnsignale:

- Nutzung gestückelter Zahlungen von nicht verbundenen Konten
- Verbindungen zu Jurisdiktionen, die mit TF-Strömen in Verbindung stehen
- Keine Prüfung der Mittelherkunft oder der endgültigen Bestimmung.

Fallstudie 5: Verkauf von Luxus-Uhren unter Verwendung von Krypto-Bargeldumwandlung

Ein Händler von Luxus-Uhren akzeptierte eine Zahlung in Höhe von 65.000 EUR, die aus einem Krypto-Wallet stammte, das über eine Kryptobörse in Fiatwährung umgewandelt

wurde. Der Kunde verlangte keine Rechnung. Nach dem Verkauf wurde dieselbe Uhr online unter einem anderen Namen erneut verkauft. Der Händler verfügte über keine internen Kontrollen zur Rückverfolgung der Herkunft der Krypto-Beträge.

Warnsignal:

- Zahlungen aus Krypto- Bargeldumwandlung
- Kein nachprüfbares Einkommen oder keine nachweisbare Kundenhistorie
- Fehlende Nachprüfbarkeit der Mittel
- Schneller Weiterverkauf von Waren zu ähnlichen Preisen.

Fallstudie 6: Offshore-Zahlung für hochwertige Gemälde

Ein Käufer kaufte ein teures Gemälde auf einer Kunstmesse und bezahlte von einem Offshore-Bankkonto. Das Gemälde wurde umgehend abgeholt. Die Due-Diligence-Prüfung hätte ergeben, dass gegen den Käufer wegen Finanzkriminalität ermittelt wurde, wobei das Offshore-Konto mit illegalen Geldern in Verbindung stand.

Warnsignale:

- Zahlung von einem Offshore-Bankkonto
- Keine Due-Diligence-Überprüfung des Käufers oder der Zahlungsquelle
- Gegen den Käufer wurde wegen Finanzkriminalität ermittelt
- Offshore-Konto stand mit illegalen Geldern in Verbindung.

Fallstudie 7: Erwerb durch Ehepartner

Der Ehepartner einer wegen Insiderhandel verurteilten Person kaufte ein Gemälde bei einer Auktion. Die Zahlung erfolgte über einen panamaischen Rechtsträger, deren Eigentümer die verurteilte Person war. Das Auktionshaus nahm die Mittel ohne angemessene Kontrolle an.

Warnsignale:

- Der Käufer war der Ehepartner einer verurteilten Person
- Die Zahlung lief über einen panamaischen Rechtsträger, der mit der verurteilten Person in Verbindung stand,
- Nutzung einer undurchsichtigen Rechtsstruktur, um den Kauf aus einem Land zu tätigen, das für Geheimhaltung und eingeschränkte Transparenz bekannt ist.

Fallstudie 8: Strukturierte Bargeldzahlungen

Ein Luxuswagenhändler verkaufte innerhalb von drei Wochen zwei Luxus-SUVs an einen Kunden. Beide Transaktionen wurden in bar unter Verwendung strukturierter Denominierungen und Multipler Payer abgewickelt. Der Käufer beantragte, dass jede Rechnung unterhalb des Meldeschwellenwerts liegen müsse. Ein Follow-up ergab, dass die Fahrzeuge über Rechtsträger in Osteuropa ausgeführt und weiterverkauft wurden.

Warnsignale:

- Wiederholte große Bargeldtransaktionen knapp unterhalb der Meldeschwelle
- Verschiedene Personen, die physische Zahlungen leisten
- Schneller Weiterverkauf und Ausfuhr der gekauften Waren.



- Fehlendes wirtschaftliches Profil zur Unterstützung der Einkäufe.

11.3.2 Risikoindikatoren für Händler

1. Indikatoren für das Kundenrisiko

- Käuferprofil (z. B. Studenten, Arbeitslose) ist nicht mit einem solch hohen Ankaufswert vereinbar
- Verwendung von Dritten oder Rechtsträgern ohne klare Erklärung
- Mangelnde Bereitschaft zur Offenlegung von WE oder Mittelherkunft
- Kunden, die aus sanktionierten Ländern oder Konfliktregionen stammen oder mit diesen in Verbindung stehen
- Mehrere hochwertige Transaktionen mit nur geringen Unterschieden bei den Waren
- Käufer, die aus Hochrisikoländern kommen oder mit Sanktionen belegt sind.

2. Geografische Risikoindikatoren

- Zur Ausfuhr in Hochrisikoländer erworbene Waren
- Beteiligung von Offshore-Finanzzentren
- Wiederkehrende Geschäfte mit Kunden in Hochrisikoländern
- Transaktionen im Zusammenhang mit Hochrisikoländern.

3. Risikoindikatoren der Lieferkanäle

- Fernkäufe ohne persönliche Treffen oder Überprüfungen
- Einsatz von virtuellen Währungen, Geschenkkarten oder Zahlungsvermittlern
- Käufer fordern keine Lieferung, Rechnungen oder Unterlagen an
- Vermittler, die im Namen nicht identifizierter Kunden handeln
- Einsatz von Vermittlern oder Maklern ohne klare Begründung.
- Ferntransaktionen ohne persönliche Überprüfung.

4. Risikoindikatoren bei Transaktionen

- Bargeldtransaktionen oberhalb des gesetzlichen Schwellenwerts
- Transaktionen knapp unterhalb der Meldeschwelle („Strukturierung“)
- Mehrere kleinere Transaktionen in einem kurzen Zeitraum
- Sofortiger Weiterverkauf oder Rückkauf derselben Ware
- Zahlungen über unabhängige Konten Dritter oder über Firmengesellschaften
- Zahlungen in bar, in Kryptowerten oder über komplexe Finanzinstrumente
- Über- oder Unterfakturierung von Waren
- Rascher Weiterverkauf der Waren nach dem Kauf.

5. Risikoindikatoren für Dienstleistungen/Waren

- Erwerb transportabler, leicht weiter verkaufter oder anonymer Waren (z. B. Uhren, Gold, Kunst)
- Hochwertige Waren, die nach dem Kauf nicht verwendet oder ausgestellt werden

- Falsche oder überhöhte Rechnungsstellung (z. B. Unter-/Überbewertung)
- Häufige Rückgabe, Umtausch oder Erstattung ohne wirtschaftliche Begründung
- Waren werden ohne klaren Zweck oder auf unbestimmte Zeit aufbewahrt
- Waren mit hoher Liquidität und Anonymität wie Gold oder Diamanten
- Fehlende Dokumentation oder Herkunft bei hochwertigen Artikeln.

11.4 Unternehmensberater (Unternehmensdienstleister)

Unternehmensberater sollten ihre Strategie an die Komplexität und Transparenz der von ihnen erbrachten Dienstleistungen anpassen. Die Unterstützung eines österreichischen Unternehmers bei der Gründung eines einzigen operativen Unternehmens mit örtlichem Personal und einer einfachen Eigentumsstruktur dürfte ein geringes Risiko darstellen. In solchen Fällen ist die Standard-CDD ausreichend.

Die Erbringung von Dienstleistungen für ausländische Kunden mit mehreren Unternehmen, Nominee-Direktoren oder Registrierungen in mehreren Jurisdiktionen dagegen birgt ein erhebliches Risiko. In diesen Fällen müssen Unternehmensberater nicht nur die Identität des Kunden, sondern auch den wirtschaftlichen Zweck der Struktur, die Legitimität der Finanzierung und die Herkunft der Beteiligten überprüfen. Wenn an den Eigentumsketten Offshore-Firmen oder Treuhandverhältnisse beteiligt sind, sollte der Unternehmensberater den tatsächlichen wirtschaftlichen Eigentümer identifizieren, unabhängige Nachforschungen durchführen und sicherstellen, dass die vollständige Dokumentation aufbewahrt wird.

Eine risikosensitive Umsetzung bedeutet auch, auf Verhaltenssignale zu achten: Ein Kunde, der unterschiedliche Anweisungen erteilt, Telefon- oder Videoanrufe vermeidet oder nur verschlüsselte Nachrichten-Apps verwendet, kann bewusst versuchen, einer Kontrolle zu entgehen. Solche Fälle erfordern eine sorgfältige Dokumentation, Aufsicht durch die Geschäftsleitung und gegebenenfalls Berichterstattung an die zentrale Meldestelle.

Unternehmensberater unterhalten häufig längerfristige Beziehungen zu Kunden durch Bürodienste, Nominee-Direktoren oder ständige Beratungsaufgaben. Von ihnen wird erwartet, dass sie die fortlaufenden Überwachungsprozesse aktiv anwenden. Dazu gehört auch, dass sie über Änderungen der Unternehmensstruktur des Kunden, seine Geschäftstätigkeit oder seine gerichtliche Exposition auf dem Laufenden sind. Wenn ein Kunde einen neuen Offshore-Anteilseigner hinzufügt oder ein Unternehmen umstrukturiert, um die wirtschaftliche Eigentümerschaft zu verschleiern, muss der Unternehmensberater das Risikoniveau neu bewerten und die Sorgfaltspflicht aktualisieren.

Unternehmensberater sollten auch regelmäßig Unternehmensaufzeichnungen, Korrespondenz und Open Source Intelligence überprüfen, um Anzeichen für kriminellen Missbrauch oder ein Sanktionsrisiko zu erkennen. Ein Mindestprüfzyklus (jährlich) für Kunden mit hohem Risiko ist ratsam, und Änderungen des Risikos sollten zu einer sofortigen Überprüfung führen.

11.4.1 Fallstudien und Warnsignale

Unternehmensberater/Unternehmensdienstleister müssen sektorspezifische Warnsignale bewerten und erkennen. Im folgenden Abschnitt werden gemeinsame Fallstudien zu Geldwäsche, Terrorismusfinanzierung und Sanktionen sowie Risikoindikatoren aus verschiedenen Quellen zusammengefasst.

Fallstudie 1: Einsatz von Vorratsgesellschaften mit Nominee-Direktoren

Ein Unternehmensberater unterstützte einen ausländischen Kunden beim Erwerb einer alten österreichischen Vorratsgesellschaft. Das Unternehmen ernannte Nominee-Direktoren und ermittelte den WE nicht. Kurz darauf eröffnete das Unternehmen mehrere Konten für den



Transfer von Geldern aus sanktionierten Ländern, die als „Beratungsgebühren“ und „Softwarelizenzen“ angegeben wurden.

Warnsignale:

- Einsatz einer Vorratsgesellschaft mit Nominee-Strukturen
- Unklarer WE
- Zahlungen aus/an mit Sanktionen belegten Länder(n)
- Keine tatsächliche gewerbliche Tätigkeit oder kein Personal.

Fallstudie 2: Gründung eines Unternehmens, das mit einer mit Sanktionen belegten Person in Verbindung steht

Ein Unternehmensberater half bei der Gründung einer Holdingstruktur und nutzte hierbei Rechtsträger in Zypern und den Britischen Jungferninseln. Die Struktur wurde später mit einem Russen in Verbindung gebracht, gegen den Sanktionen verhängt wurden. Der Unternehmensberater führte keine EDD durch, sondern verließ sich ausschließlich auf das Einführungsschreiben einer ausländischen Anwaltskanzlei.

Warnsignale:

- Nutzung von Strukturen mit mehreren Jurisdiktionen ohne wirtschaftliche Begründung
- Keine Überprüfung des WE in einer komplexen Eigentums-kette
- Einsatz eines Vermittlers (Introducer) ohne unabhängige Kontrollen
- Verbindung zu sanktionierten Personen.

Fallstudie 3: Nutzung eines virtuellen Büros und eines Strohmannes für ein kriminelles Netzwerk

Ein Unternehmensberater warb mit „vollständigen Unternehmenspaketen“ einschließlich Nominee- Direktoren, Einrichtung eines Bankkontos und E-Mail-Weiterleitung. Mehrere Kunden nutzten diese Strukturen, um große Beträge im Zusammenhang mit MwSt.-Karussellbetrug zu transferieren. Der Berater akzeptierte Bar- und Kryptozahlungen und meldete keine verdächtigen Aktivitäten.

Warnsignale:

- Kerngeschäft ist die Bereitstellung von Strukturen zur Sicherung der Anonymität
- Bar-/Kryptozahlungen
- Keine Due-Diligence-Berichte oder Meldung verdächtiger Tätigkeiten
- Kundenmuster stehen mit Straftaten in Zusammenhang.

Fallstudie 4: Hilfe bei falscher Rechnungsstellung

Ein Unternehmensberater unterstützte einen Kunden bei der Gründung mehrerer Unternehmen, um „Beratungsvereinbarungen“ durchzuführen. Die Unternehmen stellten hohe Rechnungen für fiktive Dienstleistungen an ein größeres Unternehmen aus. Diese Rechnungen wurden verwendet, um Steuerabschreibungen zu rechtfertigen und Erträge aus illegalen Arbeitspraktiken zu verschleiern. Der Berater arbeitete die Verträge aus, ignorierte jedoch die Warnsignale.

Warnsignale:

- Komplexe Strukturen ohne tatsächliche Erbringung von Dienstleistungen
- Wiederholte fiktive Transaktionen zwischen verbundenen Unternehmen
- Unverhältnismäßig hohe Dienstleistungsentgelte ohne Leistungen
- Berater, der eng in die Vertragsgestaltung eingebunden ist.

Fallstudie 5: Terrorismusfinanzierung durch Unternehmensgründung

Ein Kunde nutzte einen Unternehmensberater in Wien, um eine kleine Handelsgesellschaft zu gründen. Der Berater akzeptierte vage IDs und eröffnete die Konten. Später erhielt das Unternehmen mehrere kleine Überweisungen von verschiedenen Gebern und schleuste Gelder ins Ausland an eine Wohltätigkeitsorganisation, gegen die wegen Unterstützung terroristischer Gruppen ermittelt wurde. Der Unternehmensberater hatte keine Aufzeichnungen darüber, dass der Kunde jemals Österreich besucht hatte.

Warnsignale:

- Nutzung von Remote Onboarding und vagen Dokumenten
- Kunden, die sich nie physisch in Österreich aufhielten
- Wiederholte kleine Zahlungseingänge, die nicht mit der Geschäftstätigkeit vereinbar sind
- Begünstigte in Konfliktregionen mit bekannten TF-Verbindungen.

Fallstudie 6: Umgehung der Offenlegung des WE durch Vermittler

Ein Unternehmensberater half bei der Strukturierung einer Holdinggesellschaft mit Kreislaufigentum: Unternehmen A in Österreich stand im Eigentum des Unternehmens B in Luxemburg, das wiederum im Eigentum des Unternehmens A stand. Der gesamte Schriftverkehr erfolgte über eine Schweizer Rechtsfirma, die als „Kommunikationsbevollmächtigter“ auftrat. Die tatsächliche Kontrolle wurde von einer PEP aus einem Nicht-EU-Land ausgeübt.

Warnsignale:

- Kreislaufigentum ohne logischen Geschäftszweck
- Gesamte Korrespondenz über Bevollmächtigte oder Rechtsfirmen
- Versuche, die Offenlegung des WE im österreichischen Register zu vermeiden
- Verschleierung der Beteiligung einer PEP durch Layering.

Fallstudie 7: Schlechte CDD

Ein Unternehmensberater führte für mehrere Kunden, die über Online-Kanäle und professionelle Netzwerke eingeführt wurden, Unternehmensgründungen durch. In einem Fall stellte sich der Kunde als Immobilieninvestor vor und verlangte die schnelle Gründung von zwei Unternehmen und die Ernennung eines Nominee-Direktors. Der Berater stützte sich auf das Einführungsschreiben Dritter und führte keine aussagekräftigen Überprüfungen des Hintergrunds, des WE, der Struktur oder der Tätigkeiten des Kunden durch. Später kam es zu einem unregelmäßigen Zahlungsverhalten: Die Gebühren wurden über multiple persönliche Bankkonten und Guthabekarten bezahlt. Anschließend wurden die Unternehmen dazu

verwendet, ungewöhnlich große Immobilieneinlagen zu tätigen, gefolgt von sofortigen Auszahlungen an unabhängige Parteien.

Warnsignale:

- Forderung einer schnellen Unternehmensgründung mit Hinweis auf Dringlichkeit oder Absicht, die Prüfung zu umgehen
- Einsatz eines Nominee-Direktors zur Verschleierung der tatsächlichen Kontrolle
- Kundeneinführung über Online-Kanäle
- Berufung auf Einführungsschreiben Dritter
- Keine Kontrolle der wirtschaftlichen Eigentümer oder der Geschäftstätigkeit des Kunden
- Gebühren, die über multiple persönliche Bankkonten und Guthabekarten bezahlt werden
- Ungewöhnliche Finanztätigkeit der Unternehmen kurz nach deren Gründung
- Große Einlagen, gefolgt von sofortigen Auszahlungen an unabhängige Parteien.

Fallstudie 8: Schwache interne Verfahren während der Unternehmensgründung

Ein Unternehmensberater, der Unternehmensgründungen anbietet, bearbeitete eine Welle neuer Kundenanfragen eines außerhalb der EU ansässigen Empfehlungsnetzwerkes. Die meisten Kunden forderten eine schnelle Gründung von Unternehmen in Österreich und führten vage Geschäftszwecke wie „Beratung“ oder „internationaler Handel“ an. Die Risikobewertungen waren allgemein gehalten und für alle Kunden identisch. Bei Kunden aus Hochrisikoländern wurde kein EDD durchgeführt, und die WE-Erklärungen wurden ohne Überprüfung akzeptiert. Im Laufe der Zeit versäumten es mehrere Kunden, Finanzinformationen einzureichen oder grundlegende Anfragen zu beantworten. Einige Unternehmen standen später mit ungewöhnlich hohen Inbound-Transfers aus Kryptobörsen in Verbindung.

Warnsignale:

- Mehrere Kunden in kurzer Zeit aus demselben Empfehlungsnetzwerk
- Forderung einer schnellen Unternehmensgründung ohne glaubhafte Begründung
- Angabe vager Geschäftszwecke (z. B. „Beratung“, „internationaler Handel“)
- Kunden aus Hochrisikogebieten
- Annahme der WE-Erklärungen ohne unabhängige Überprüfung
- Versäumnis der Kunden, Finanzinformationen einzureichen oder den Kontakt aufrechtzuerhalten
- Unternehmen erhalten hohe Inbound-Transfers aus Kryptobörsen.

Fallstudie 9: Nominee-Direktor

Ein Unternehmensberater spezialisierte sich auf beschleunigte Unternehmensgründungen. Ein und derselbe Nominee-Direktor wurde in über 100 Unternehmen geführt, von denen viele die gleiche Adresse und den gleichen Geschäftszweck hatten. Die Kunden waren häufig im Ausland ansässig und legten nur eine minimale Dokumentation vor. Bei der Überprüfung wurde festgestellt, dass einige dieser Unternehmen dazu genutzt wurden, um Erträge aus MwSt.-Karussellbetrug zu waschen und gefälschte Rechnungen für „Beratungsdienste“ auszustellen.

Warnsignale:

- Wiederholter Einsatz einer Person als Nominee-Direktor.
- Mehrere Rechtsträger, die unter identischen Adressen registriert sind
- Fehlende Geschäftstätigkeit oder fehlende Finanzunterlagen für die Unternehmen
- Ausländische Kunden, die ähnliche Dokumentationsvorlagen verwenden
- Mantelgesellschaften ohne wirtschaftliche Begründung.

11.4.2 Risikoindikatoren für Unternehmensberater

1. Indikatoren für das Kundenrisiko

- Kunden, die nicht bereit sind, den WE offenzulegen oder unklarer WE
- Kunden, die auf Strohmännern, Mantelgesellschaften oder Kreislaufeigentum bestehen
- Einsatz von Strohmännern, Bevollmächtigten oder gesetzlichen Vertretern als wirtschaftlicher Eigentümer
- Beteiligung von PEP oder Personen mit hohem Risiko ohne erweiterte Sorgfaltspflicht
- Kunden aus Sektoren mit historisch hohem ML-Risiko (z. B. Baugewerbe, Kryptowerte, Import/Export).

2. Geografische Risikoindikatoren

- Kunden oder Transaktionen, die mit Hochrisikoländern in Verbindung stehen
- Ausländische Kunden mit minimaler Dokumentation.

3. Risikoindikatoren der Lieferkanäle

- Gesamte Abwicklung online oder über Intermediäre
- Einsatz von Vermittlern (Introducer) ohne unabhängige Überprüfung
- Verwendung ungewöhnlicher Adressen, virtueller Büros oder E-Mail-Weiterleitung als eingetragener Geschäftssitz
- Keine persönliche Interaktion.

4. Risikoindikatoren bei Transaktionen

- Bezahlung der Dienstleistung in bar, in Kryptowerten oder über Konten unabhängiger Dritter
- Strukturierung von Unternehmen für fiktive oder kreislauforientierte Rechnungsstellungssysteme
- Ungewöhnliche Häufigkeit von Anträgen auf Eintragung und Auflösung
- Fehlende Geschäftspläne oder wirtschaftliche Begründung für die geschaffenen Strukturen.

5. Risikoindikatoren für Dienstleistungen/Waren

- Nutzung von Diensten zur Stärkung der Anonymität (z. B. Nominee-Direktoren, Mantelgesellschaften)
- Aufbau komplexer Strukturen ohne klaren operativen Zweck
- Beteiligung an der Gründung von Trusts, Stiftungen für gebietsfremde Kunden
- Vermeidung oder Verzögerung bei der Registrierung von Unternehmen in österreichischen WE-Registern
- Große Anzahl von Unternehmensgründungen mit demselben Direktor oder derselben Adresse.