

# **Nationale Risikoanalyse der Geldwäscherei und Terrorismusfinanzierung**

## **Impressum**

Medieninhaber, Verleger und Herausgeber:

Bundesministerium für Finanzen, Johannesgasse 5, 1010 Wien

Wien, 2021. Stand: 11. Mai 2021

## **Copyright und Haftung:**

Auszugsweiser Abdruck ist nur mit Quellenangabe gestattet, alle sonstigen Rechte sind ohne schriftliche Zustimmung des Medieninhabers unzulässig.

Es wird darauf verwiesen, dass alle Angaben in dieser Publikation trotz sorgfältiger Bearbeitung ohne Gewähr erfolgen und eine Haftung des Bundesministeriums für Finanzen und der Autorin/des Autors ausgeschlossen ist. Rechtausführungen stellen die unverbindliche Meinung der Autorin/des Autors dar und können der Rechtsprechung der unabhängigen Gerichte keinesfalls vorgreifen.

Rückmeldungen: Ihre Überlegungen zu vorliegender Publikation übermitteln Sie bitte an [email@bmf.gv.at](mailto:email@bmf.gv.at).

## Vorwort



Sehr geehrte Damen und Herren,

Geldwäscherei und Terrorismusfinanzierung sind auch in den letzten Jahren äußerst prägnante Herausforderungen geblieben. Dabei zeigte sich wiederholt die Wichtigkeit wirksamer Präventionsmaßnahmen für den Schutz der Finanzmärkte und der Volkswirtschaft als Ganze vor inkriminierten Geldern. Effektive Kontrollsysteme stärken zudem die Reputation der Unternehmen und tragen damit zur Wettbewerbsfähigkeit des Standorts Österreich bei.

Kernstück der internationalen und europäischen Standards zur Geldwäschebekämpfung ist der risikobasierte Ansatz, welcher die Maßnahmen zur Verhinderung von Geldwäscherei und Terrorismusfinanzierung kennzeichnet. Wichtigstes Element des risikobasierten Ansatzes ist die Erstellung von Risikoanalysen auf supranationaler und nationaler Ebene sowie für die betroffenen Wirtschaftssektoren und Unternehmen.

Die vorliegende Nationale Risikoanalyse stellt daher eine wichtige Grundlage der Maßnahmen zur Prävention von Geldwäscherei und Terrorismusfinanzierung dar. Sie identifiziert die Risiken der betroffenen Sektoren anhand der Analyse der vorherrschenden Gefahren und Schwachstellen und soll es Behörden und Verpflichteten ermöglichen, ihre Ressourcen zielgerichtet einzusetzen und effektive Präventionsmaßnahmen zu ergreifen. Die Nationale Risikoanalyse ist das gemeinsame Ergebnisdokument aller mit der Prävention und Bekämpfung von Geldwäscherei und Terrorismusfinanzierung in Österreich befassten Behörden. Sie wurde auf Basis ausführlicher Sektoranalysen verfasst.

Die einzelnen Analysen zeigen eine differenzierte Risikolandschaft auf. Risiken der Geldwäscherei und Terrorismusfinanzierung unterscheiden sich in Bezug auf einzelne Produkte und Dienstleistungen, innerhalb sowie zwischen Sektoren.

Die Nationale Risikoanalyse soll außerdem zu einem besseren Risikoverständnis sämtlicher betroffener Behörden und des Privatsektors beitragen und dadurch insgesamt zu einer effektiveren Bekämpfung von Geldwäscherei und Terrorismusfinanzierung in Österreich führen. Das Bundesministerium für Finanzen bekennt sich zur Umsetzung der internationalen und europäischen Standards zur Geldwäschebekämpfung und deren stetiger Fortentwicklung mit seinen europäischen und internationalen Partnern.

Mag. Harald Waiglein, MSc.

Sektionschef der Sektion III - Wirtschaftspolitik, Finanzmärkte und Zölle

## Inhalt

<b>Vorwort</b> .....	<b>3</b>
<b>Einleitung</b> .....	<b>5</b>
1. Zielsetzungen der Nationalen Risikoanalyse .....	5
2. Erstellung der Nationalen Risikoanalyse .....	6
3. Methodologie .....	7
<b>Vortaten zur Geldwäscherei</b> .....	<b>8</b>
<b>Betrugsbekämpfung, Steuer, Zoll und Geldwäscherei</b> .....	<b>14</b>
<b>Bedrohungsszenarien der Terrorismusfinanzierung</b> .....	<b>22</b>
<b>Risiken der Proliferationsfinanzierung</b> .....	<b>26</b>
<b>Risiko juristischer Personen und Trusts</b> .....	<b>28</b>
<b>Sektorrisikoanalyse Finanzsektor</b> .....	<b>42</b>
<b>Risiko der Verletzung von Sanktionsmaßnahmen</b> .....	<b>74</b>
<b>Risiko der Umgehung von EU-Finanzsanktionen gegen Terrorismusfinanzierung</b> .....	<b>76</b>
<b>Sektorrisikoanalyse Rechtsanwälte</b> .....	<b>80</b>
<b>Sektorrisikoanalyse Notariat</b> .....	<b>88</b>
<b>Sektorrisikoanalyse Wirtschaftstreuhandberufe</b> .....	<b>98</b>
<b>Sektorrisikoanalyse Bilanzbuchhaltung</b> .....	<b>111</b>
<b>Sektorrisikoanalyse Glücksspiel</b> .....	<b>116</b>
<b>Sektorrisikoanalyse Gewerbe</b> .....	<b>126</b>
<b>Schlusswort</b> .....	<b>136</b>
<b>Abkürzungsverzeichnis</b> .....	<b>137</b>

# Einleitung

## 1. Zielsetzungen der Nationalen Risikoanalyse

Die **Grundlage aller Maßnahmen** zur Prävention von Geldwäscherei und Terrorismusfinanzierung der Behörden und Verpflichteten des Privatsektors ist der **risikobasierte Ansatz**. Dieser setzt ein **umfassendes Verständnis** der **nationalen Risikolandschaft** voraus.

Ziel der Nationalen Risikoanalyse ist es, eine solche Grundlage zu schaffen.

**Gemäß § 3 Abs. 3 Finanzmarkt-Geldwäschegesetz (FM-GwG) und Art. 7 Abs. 4 der 5. Geldwäschere Richtlinie (GW-RI)** dient die Nationale Risikoanalyse folgenden Zwecken:

- **Verbesserung des Systems** zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung, insbesondere zur **Ermittlung aller etwaigen Bereiche**, in denen die Verpflichteten **verstärkte Maßnahmen** anwenden müssen und zur **Empfehlung der zu treffenden Maßnahmen**.
- **Identifikation von Sektoren oder Bereichen** mit **geringem** oder **erhöhtem Risiko** für Geldwäscherei und Terrorismusfinanzierung.
- **Identifikation von Risiken** der Geldwäscherei und Terrorismusfinanzierung in Bezug auf die Entwicklung von **neuen Produkten** und **neuen Geschäftspraktiken** inklusive **neuer Vertriebsmechanismen** und der Nutzung von **neuen oder sich entwickelnden Technologien** sowohl für **neue** als auch **bereits existierende Produkte**.
- **Zuteilung von Ressourcen** und **Prioritätensetzung** bei den Ressourcen für die Bekämpfung von Geldwäscherei und Terrorismusfinanzierung.
- **Sicherstellung**, dass **für jeden Sektor oder Bereich** den Risiken der Geldwäscherei und Terrorismusfinanzierung entsprechende angemessene Regelungen festgelegt werden.
- Umgehende **Versorgung der Verpflichteten mit angemessenen Informationen**, damit diese ihre eigene Bewertung des Risikos der Geldwäscherei und Terrorismusfinanzierung leichter vornehmen können.
- Meldung der **institutionellen Struktur** und der **groben Verfahren der eigenen Systeme** zur Bekämpfung der Geldwäsche und Terrorismusfinanzierung, unter anderem in Bezug auf die zentralen Meldestellen, Steuerbehörden und Staatsanwälte, sowie die zugewiesenen Human- und Finanzressourcen, soweit diese Informationen zur Verfügung stehen.

- Meldung der **nationalen Anstrengungen und Ressourcen** (Arbeitskräfte und Finanzmittel), die zur Bekämpfung der Geldwäsche und Terrorismusfinanzierung zur Verfügung gestellt wurden.

Die Bundesminister / Bundesministerinnen für Finanzen, Justiz, für Inneres, für Digitalisierung und Wirtschaftsstandort, für europäische und internationale Angelegenheiten sowie die FMA und die Oesterreichische Nationalbank haben im Rahmen ihrer Zuständigkeit **entsprechende Maßnahmen zur Verwirklichung dieser Zwecke** zu setzen.

## 2. Erstellung der Nationalen Risikoanalyse

Die **1. Nationale Risikoanalyse Österreich (NRA I)** datiert mit **April 2015**. Seitdem entwickelte sich der europäische und internationale Rechtsrahmen stetig. Durch die Länderprüfung Österreichs durch die Financial Action Task Force (FATF) in den Jahren 2015 und 2016 ergaben sich neue Empfehlungen für die Durchführung der Nationalen Risikoanalyse. Zusätzlich ist eine stetige **Entwicklung der Risikolage** und die **Ausdehnung der Materiengesetze** auf neue Verpflichtete zu verzeichnen. Eine Aktualisierung ist somit angebracht.

**Ausgangspunkt** der Nationalen Risikoanalyse ist das **Nationale Koordinierungsgremium zur Entwicklung von Maßnahmen und Strategien zur Verhinderung der Geldwäscherei und Terrorismusfinanzierung**, das beim Bundesminister für Finanzen eingerichtet ist. Dieses setzt sich aus allen relevanten Ressorts und Behörden zusammen.

Gemäß **§ 3 Abs. 2 FM-GwG** hat das Koordinierungsgremium zur Entwicklung von Maßnahmen und Strategien zur Verhinderung der Geldwäscherei und Terrorismusfinanzierung eine Nationale Risikoanalyse zu erstellen und laufend zu aktualisieren. Die **Grundlage der Nationalen Risikoanalyse** stellen die **Beiträge der Mitglieder** dar, die diese im Rahmen ihrer jeweiligen Zuständigkeit zu erstellen haben.

Der Erstellungsprozess erfolgte in drei Schritten.

- 1) Auf Basis einer **gemeinsamen Vorlage und Methodologie** erstellten die Mitglieder einen **Erstentwurf ihrer Sektorrisikoanalysen**. Dabei handelt es sich um **Ergebnisdokumente**, in denen die Schlussfolgerungen und Ergebnisse von **ausführlichen Voralysen** abgebildet sind. Dieser Ansatz und die damit einhergehende Kompaktheit der Beiträge tragen einer **Empfehlung der FATF** aus der letzten Länderprüfung Österreichs Rechnung.
- 2) Die Erstentwürfe wurden an das **Bundesministerium für Inneres** zum **Abgleich mit operativen Erkenntnissen** übermittelt. Parallel dazu erhielten die relevanten **VertreterInnen des Privatsektors** den Berichtsentwurf zur Kommentierung.

- 3) Unter **Berücksichtigung der Rückmeldungen** des Bundesministeriums für Inneres und des Privatsektors erfolgte die **Erstellung der Letztentwürfe** und deren Konsolidierung in einem Gesamtdokument.

### 3. Methodologie

Die **aktualisierte Nationale Risikoanalyse (NRA II)** soll die Empfehlungen des FATF Länderberichts 2016 sowie die Vorgaben der 4. und 5. GW-RI berücksichtigen.

Die Sektorrisikoanalysen stützen sich auf die **Methodologie der Supranationalen Risikoanalyse (SNRA)**, die gemäß Art. 6 Abs. 1 der 5. GW-RI von der Europäischen Kommission zu erstellen ist. Eine umfassende Darstellung der zugrundeliegenden Methodologie ist in dem Staff Working Document (SWD) der SNRA 2017, S 233 ff, enthalten. Die aktuellste SNRA, deren Risikoeinschätzungen im Rahmen der Sektorrisikoanalysen berücksichtigt wurden, stammt aus dem Jahr 2019.

Im Folgenden werden die Kernpunkte dieses methodologischen Ansatzes kurz umrissen. Der **Bedrohung** und **Verletzbarkeit** für Geldwäscherei und Terrorismusfinanzierung wird jeweils ein **Wert** zugewiesen (**niedrig/mittel/hoch/sehr hoch**), die den Werten 1 - 4 (lowly significant/moderately significant/significant/very significant) der SNRA korrespondieren. Die **Einstufung von Bedrohung und Verletzbarkeit** folgt der Beschreibung des SWD 2017, S 248 ff. Als Datengrundlage dienen quantitatives Zahlenmaterial und im Rahmen der Aufsichtstätigkeit gewonnene Erkenntnisse. Anschließend werden die bestehenden risikomindernden Maßnahmen geschildert.

Das Gesamtrisiko berechnet sich nach der Formel: **40% Bedrohung + 60% Verletzbarkeit – risikomindernde Maßnahmen = Gesamtrisiko.**

Wie die Methodologie der SNRA nimmt die Nationale Risikoanalyse an, dass die **Verletzbarkeit** einen **stärkeren Einfluss auf das Gesamtrisiko** als die Bedrohung ausübt und daher stärker zu gewichten ist.

Abschließend leiten die Sektorrisikoanalysen **Empfehlungen** aus den erlangten Erkenntnissen ab. Da die Nationale Risikoanalyse ein Behördendokument ist, richtet sich diese nur an **Behörden**. Es steht den zuständigen Behörden weiterhin frei, auf Basis der erlangten Erkenntnisse im Rahmen ihrer Aufsichtstätigkeit weitere Maßnahmen in Bezug auf ihre Verpflichtete zu formulieren.

Zur leichteren Lesbarkeit der Nationalen Risikoanalyse wurde stets die männliche Form personenbezogener Hauptwörter gewählt. Frauen und Männer werden jedoch gleichermaßen angesprochen.

# Vortaten zur Geldwäscherei

## Analyse der Vortaten zur Geldwäscherei

### Allgemeine Informationen

#### Der Begriff der „Vortat“

Der vorliegende Beitrag beleuchtet das Delikt Geldwäscherei (§ 165 StGB) aus der Perspektive der geldwäschetauglichen Vortaten und stellt – gestützt auf mehrere Quellen – jene Vortaten dar, die besonders häufig im Zusammenhang mit Geldwäscherei stehen und deren Begehungsrisiko daher besonders hoch ist.

Gemäß § 165 Abs. 1 StGB ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen, wer Vermögensbestandteile, die aus bestimmten Straftaten herrühren, verbirgt oder ihre Herkunft verschleiert. Eine zentrale Funktion der Kriminalisierung dieser als „Geldwäscherei“ definierten Handlung liegt darin, die Nutzung illegal erlangter Vermögenswerte zu erschweren, indem auch das Verbergen oder Verschleiern ihrer Herkunft pönalisiert wird.

Geldwäscherei ist ein sogenanntes Anschlussdelikt. Das bedeutet, dass für die Strafbarkeit (mit Ausnahme des § 165 Abs. 3 StGB) jedenfalls auch der Nachweis **bestimmter Vortaten erforderlich** ist. Der Vortaten-Katalog des § 165 Abs. 1 StGB wurde in der Vergangenheit stetig erweitert. Mittlerweile ist das Waschen jeglicher Vermögensbestandteile strafbar, die aus Handlungen stammen, die mit mehr als einjähriger Freiheitsstrafe bedroht sind oder aus Vergehen nach den §§ 223, 229, 289, 293, 295 StGB oder §§ 27 oder 30 SMG hervorgehen.

Für die Strafbarkeit der Geldwäscherei ist es unerheblich, ob sie durch dieselben Täter begangen wird wie die Vortat (sogenannte Eigengeldwäsche) oder ob die Geldwäscherei durch Dritte erfolgt. Im Gegensatz zu Eigengeldwäschern machen sich Dritte gemäß § 165 Abs. 2 StGB aber nicht erst strafbar, wenn sie geldwäschetaugliche Vermögenswerte verbergen oder ihre Herkunft verschleiern, sondern bereits dann, wenn sie derartige Vermögenswerte wissentlich an sich bringen, verwahren, anlegen, verwalten, umwandeln, verwerten oder übertragen.

Zuletzt macht sich gemäß § 165 Abs. 3 StGB auch strafbar, wer wissentlich Vermögensbestandteile an sich bringt, verwahrt, anlegt, verwaltet etc., die der Verfügungsmacht einer kriminellen Organisation oder einer terroristischen Vereinigung unterliegen. Wegen der hohen kriminellen Energie derartiger Gruppierungen und der von ihr ausgehenden Gefahren kommt es bei dieser Begehungsform auf das Vorliegen einer geldwäschereitauglichen Vortat nicht an.

#### Datenbasis für die Risikobewertung

Die A-FIU (Financial Intelligence Unit) ist Teil der Sicherheitsbehörden und stützt die folgende Analyse daher auf folgende Quellen: Zum einen erhält die A-FIU als zentrale Geldwäschemeldestelle Verdachtsmeldungen der meldepflichtigen Berufsgruppen und kann aus den darin dargestellten Sachverhalten, die auf bestimmte Vortaten schließen lassen, das Risiko für deren Begehung ableiten (Grafik 1). Zum anderen stützt sich die Analyse auf Daten der Kriminalstatistik aus den Jahren 2018 bis 2020 (Grafik 2). Aus dieser lassen sich jene Straftaten bestimmen, zu denen am häufigsten im Zusammenhang mit dem Grunddelikt

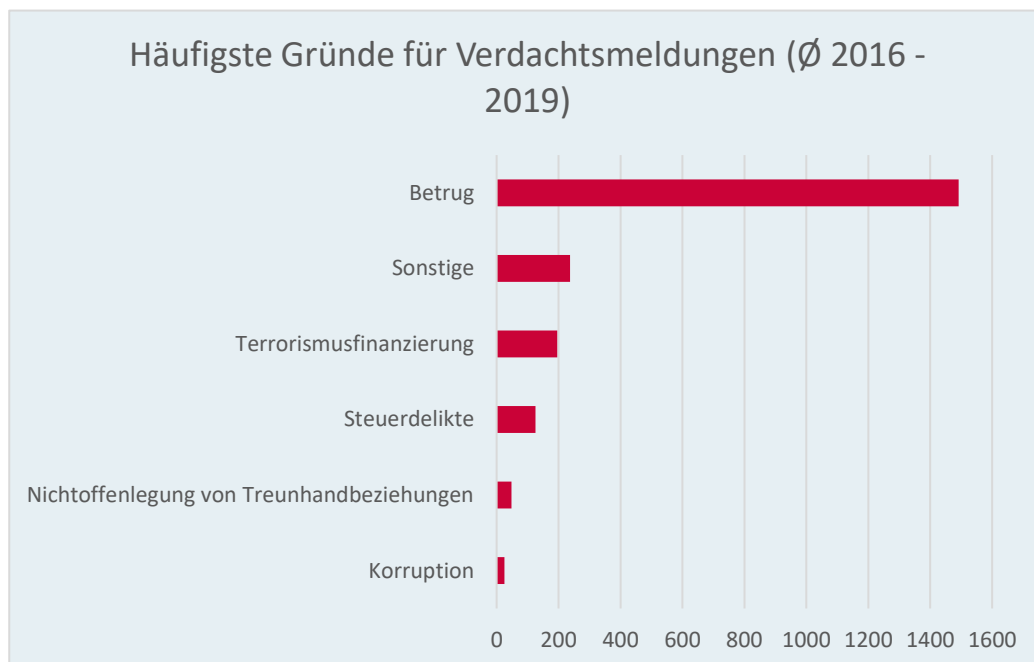


Geldwäscherei ermittelt (nicht verurteilt!) wurde. Diese Statistik weist daher auch Straftaten aus, die den Begriff der „Vortat“ iSd § 165 StGB nicht erfüllen; weil sie z.B. nicht mit einer mehr als einjährigen Freiheitsstrafe bedroht sind (dazu gehört z.B. ein einfacher Diebstahl).

Darüber hinaus berücksichtigt die folgende Analyse auch Kriminalitätsfelder, zu denen die A-FIU kaum Verdachtsmeldungen erhält, aber bei denen eine hohe Dunkelziffer anzunehmen ist. Dabei handelt es sich vor allem um Suchtmitteldelikte bzw. um Straftaten im Bereich der organisierten Kriminalität.

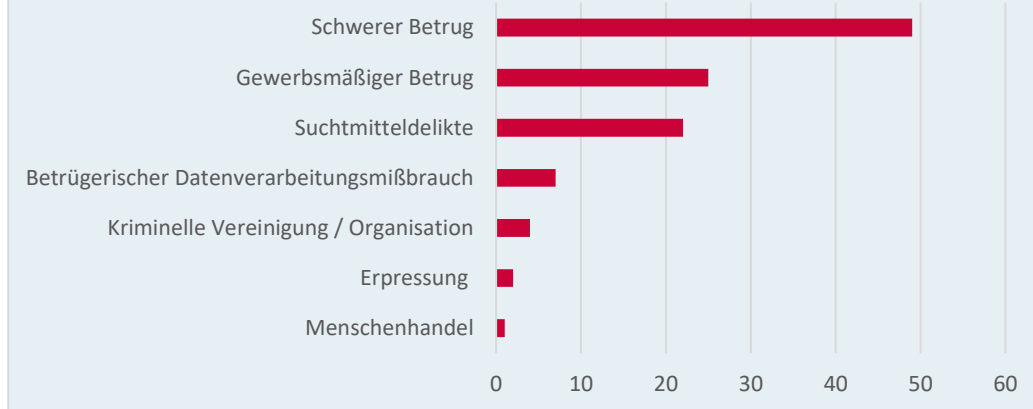
Nicht beschrieben sind die Daten zu Vortaten, für deren Ermittlung andere Stellen zuständig sind; dazu gehören die Vortaten aus den Bereichen der Steuerdelikte und der Korruption sowie die Terrorismusfinanzierung.

Die folgende Statistik der Verdachtsmeldungen und die Daten der polizeilichen Kriminalstatistik zeigt jene Straftaten, die am häufigsten in Verbindung mit Geldwäscherei stehen.



Grafik 1

## Häufigste Delikte im Zusammenhang mit Ermittlungen wegen Geldwäscherei (Ø von 2018-2020)



Grafik 2

### Häufigste Vortaten zur Geldwäscherei: Betrugs kriminalität

Laut der polizeilichen Kriminalstatistik wurde in den vergangenen drei Jahren bei Ermittlungen wegen Geldwäscherei im Durchschnitt 49 Mal ein Zusammenhang mit schwerem Betrug (§ 147 StGB) angenommen. Im gleichen Zeitraum wurde in durchschnittlich rund 26 Fällen ein Zusammenhang mit gewerbsmäßigem Betrug (§ 148 StGB) und in sieben Fällen mit betrügerischem Datenverarbeitungsmissbrauch (§ 148a StGB) festgestellt.

Die Häufigkeit von Betrugsdelikten deckt sich auch mit Erkenntnissen, die die A-FIU aus den bei ihr eingelangten Verdachtsmeldungen ableitet, da Verdachtsmeldungen zur Geldwäscherei am häufigsten wegen des Verdachts von Betrugshandlungen erstattet werden: Finanz- und Kreditinstitute haben lange Erfahrung mit diesem Kriminalitätsphänomen und erkennen daher die Vorgehensweisen, die auf Betrugshandlungen schließen lassen.

Betrügereien finden mittlerweile vorwiegend im Internet statt. Durch die Demokratisierung des Internets verfügt heute fast jeder über einen Internetzugang und immer mehr Bereiche des täglichen Lebens spielen sich in der virtuellen Welt ab; das Risiko, Opfer von Internetbetrug zu werden, ist daher entsprechend hoch. Aufgrund der bei der A-FIU erstatteten Verdachtsmeldungen besonders häufig festzustellen sind mittlerweile der betrügerische Verkauf von Waren und Dienstleistungen, die nicht geliefert werden, oder Vermögensschädigungen im Wege von betrügerisch erlangten Kontodaten, die verwendet werden, um Gelder des Opfers abzudiversifizieren.

Die beschriebenen Betrugsstrukturen sind oft auf die Unbedarftheit der Opfer zurückzuführen, allerdings sind auch vermehrt Vorgehensweisen festzustellen, die auch erfahrene Menschen täuschen können. Dazu gehören insbesondere der Anlagebetrug und CEO Fraud: Dabei veranlassen die Täter Unternehmen, unter Vorgabe, ein führender Mitarbeiter zu sein und indem ein zeitlicher Druck aufgebaut wird, Zahlungen auf bestimmte Konten durchzuführen. Durch das autoritäre Auftreten lassen sich Mitarbeiter täuschen und sie weisen entsprechende Transaktionen an.

#### **Häufigste Vortaten zur Geldwäscherei: Erpressung**

In letzter Zeit lässt sich im Zusammenhang mit Internetkriminalität und Geldwäscherei auch ein neuer Trend zur Vortat der Erpressung (§§ 144 ff StGB) erkennen.

Häufig wählen die Täter den Weg, mit Verschlüsselungsprogrammen die persönlichen Daten oder ganze Betriebssystem der Opfer zu verschlüsseln (Ransomware-Attacke) oder durch Distributed Denial of Service (DDoS)-Attacken die Verfügbarkeit von Servern zu unterbinden. Während dieser Angriffe werden die Entschlüsselung der Daten oder das Ende der DDoS-Attacke in Aussicht gestellt und so von den Opfern Geld erpresst.

#### **Häufigste Vortaten zur Geldwäscherei: Suchtkriminalität**

Häufig treten im Zusammenhang mit Ermittlungen zur Geldwäscherei auch Straftaten gegen das Suchtmittelgesetz auf, deren Begehungsrisiko daher hoch einzuschätzen ist. Die polizeiliche Kriminalstatistik der letzten drei Jahre weist durchschnittlich 22 Fälle von Geldwäscherei jährlich aus, in deren Zusammenhang auch zu unerlaubtem Umgang mit Suchtgiften gemäß § 27 Suchtmittelgesetz (SMG) und zur Vorbereitung von Suchtgifthandel gemäß § 28 SMG ermittelt wurde.

Die Deliktshäufigkeit und das damit verbundene hohe Risiko sind unter anderem auf die weite Verbreitung von Suchtmitteln und deren relativ hohe Verfügbarkeit zurückzuführen. Die Deliktshäufigkeit spiegelt sich indes nicht in den bei der A-FIU eingelangten Verdachtsmeldungen wider; die Gründe hierfür sind, dass es sich bei § 28 SMG (Vorbereitung von Suchtgifthandel) um ein bloßes Vorbereitungsdelikt handelt, und dass bei unerlaubtem Umgang mit Suchtgift (§ 27 SMG) oft geringere Entgelte und Zahlungen erfolgen, deren Abwicklung meist ohne Inanspruchnahme von Dienstleistungen meldepflichtiger Berufsgruppen erfolgt. Transaktionen in Verbindung mit Suchtmitteln laufen vielfach über das informelle Transaktionssystem Hawala.

#### **Häufigste Vortaten zur Geldwäscherei: Organisierte Kriminalität**

Eine besondere Form der Geldwäsche begeht, wer wissentlich Vermögensbestandteile an sich bringt, verwahrt, anlegt, verwaltet etc., die der Verfügungsmacht einer kriminellen Organisation oder einer terroristischen Vereinigung unterliegen (§ 165 Abs. 3 StGB); auf eine bestimmte Vortat kommt es dabei nicht an. Die polizeiliche Kriminalstatistik der vergangenen drei Jahre weist jährlich durchschnittlich vier Fälle von Ermittlung wegen Geldwäscherei aus, in denen der Verdacht im Raum stand, dass Vermögensbestandteile einer kriminellen Vereinigung bzw. Organisation gewaschen wurden. Trotz dieser – absolut betrachtet – niedrigen Zahlen ist wegen der hohen kriminellen Energie derartiger Gruppierungen und der von diesen Gruppierungen ausgehenden Gefahren von einem hohen Risiko auszugehen.

Dass keine der bei der A-FIU eingelangten Verdachtsmeldungen mit der Annahme des Vorliegens einer kriminellen Organisation begründet ist, liegt wohl daran, dass der Zusammenhang der Transaktion mit einem bestimmten Organisationstypus oder -grad – anders als eine bestimmte Vortat – noch schwerer erkennbar ist.

#### **Häufigste Vortaten zur Geldwäscherei: Menschenhandel und Schlepperei**

Regelmäßig finanzieren sich kriminelle Organisationen auch durch die Begehung von Menschenhandel und Schlepperei. Zwangsprostitution bzw. der Schmuggel von Migranten stellen lukrative Einnahmequellen für kriminelle Organisationen dar.

Opfer von Menschenhandel stammen oft aus vulnerablen Bevölkerungsschichten und sind hohem Zwang ausgesetzt, sie haben daher häufig Angst davor, überhaupt Anzeige zu erstatten. Im Falle von (erfolgreicher) Schlepperei gibt es keine Opfer im engeren Sinn und die Geschleppten erstatten selten eine (Selbst-)anzeige. Die Dunkelziffer dieses Deliktsbereichs ist dementsprechend hoch. Dennoch ist aufgrund des erheblichen Schadens für die Gesellschaft und die Opfer von einem hohen Risiko auszugehen.

Ein anderes Bild hingegen zeigt – und bestätigt daher indirekt die Annahme einer hohen Dunkelziffer in diesem Deliktsbereich – die Analyse einiger Verdachtsmeldungen, die bei der A-FIU einlangen: Die Kategorie „Sonstige“ der Grafik 1 enthält auch Verdachtsmeldungen, die aufgrund der Befürchtung erstattet wurden, dass die darin gemeldeten Transaktionen nicht freiwillig, sondern unter Zwang erfolgt sein könnten. Wenngleich die Analysen dieser Verdachtsmeldungen oft nicht den Beweis der Nötigung erbringen können, so lassen sie doch regelmäßig vermuten, dass die Transaktionen durch Prostituierte durchgeführt werden. Aufgrund der hohen Transaktionssummen und der Häufigkeit solcher Überweisungen ist nicht auszuschließen, dass sie die Gelder für einen Dritten überweisen.

### **Häufigste festgestellte Methoden der Geldwäscherei**

#### **Kryptowährungen**

Trotz der beachtlichen Kursschwankungen sind Kryptowährungen weiterhin ein bewährtes Mittel der Geldwäsche. Dabei kann inkriminiertes Geld relativ einfach über Handelsplattformen in Kryptowährungen getauscht werden. Gegen Entgelt lassen sich Transaktionen mit Hilfe von sogenannten Mixern oder Tumbler so verschleiern, dass die Herkunft nicht mehr nachgewiesen werden kann. Dies stellt für Strafverfolgungsbehörden generell, so auch für die A-FIU, eine besondere Herausforderung dar. Mittlerweile besteht auch die Möglichkeit, Kryptowährung auf Prepaid-Karten zu laden, um so direkt mit dieser in der Realwirtschaft verfügen zu können.

#### **Money Mules**

Die Entwicklungen im Bereich der Finanzagenten bleiben weiterhin besorgniserregend. Finanzagenten sind Personen, die häufig von kriminellen Organisationen rekrutiert werden, um illegal erwirtschaftete Vermögenswerte weiter zu transferieren.

Die Kontaktaufnahme zu potenziellen Finanzagenten erfolgt vorwiegend über das Internet durch Stellenangebote, die lukrative Verdienste bei geringem Aufwand in Aussicht stellen. Aufgabe der angeworbenen Personen ist es, Überweisungen auf ihrem Konto zu empfangen und auftragsgemäß weiterzuleiten. Die Zielkonten sind global verstreut. Durch den internationalen Transfer und die Einbindung vieler Identitäten entsteht die von den Tätern gewollte Verschleierung.

#### **Hawala**

Hawala ist ein weltweit verbreitetes informelles Transaktionssystem, dessen Wurzeln im Orient liegen und bis ins frühe Mittelalter reichen. Es basiert auf Vertrauen, das durch gemeinsame sprachliche, ethnische und religiöse Identifikationsmerkmale gebildet wird. Dieses System hat auch im Internetzeitalter und dem damit einhergehenden Online-Banking Bestand. Generell wird es von Personen mit Migrationshintergrund und deren zurückgelassenen Familien speziell in Entwicklungs- und Krisengebieten häufig in Anspruch genommen. Genutzt wird es häufig für sogenannte „Remittances“ (Rücküberweisungen in die Heimatländer). Auf diese Weise können Gelder rasch und anonym auch in entlegene Gebiete ohne entsprechende Infrastruktur und Anbindung an den internationalen Zahlungsverkehr, transferiert werden. Dabei werden keine digitalen Spuren hinterlassen.

Hohes Potential zur Nutzung des Hawalasytems haben vor allem jene Branchen, die im täglichen Geschäftsbetrieb bargeldintensive Geschäfte abwickeln und regelmäßig ausländische Geschäftsbeziehungen pflegen, die mit einer dementsprechend großen Anzahl von damit verbundenen Auslandstransaktionen einhergehen.

Neuere Erkenntnisse deuten darauf hin, dass das Hawalasytem in Österreich besonders im Bereich des Suchmittelhandels und der Schlepperei genutzt wird.

#### **Urkundenfälschung**

Urkundenfälschung ist zwar in § 165 StGB ausdrücklich als Vortat zur Geldwäscherei erwähnt, in der Praxis sind es jedoch selten die mittels Urkundenfälschung verdienten Vermögenswerte, die den Geldwäschereiverdacht begründen. Vielmehr dient die Urkundenfälschung meist als Mittel der Begehung der Geldwäscherei. Täter legen zum Beispiel bei Kontoöffnungen falsche Ausweisdokumente vor. Hierzu werden oftmals gestohlene Reisepässe oder Personalausweise verwendet und mit dem Bild des Täters versehen.

Besonders häufig ist in letzter Zeit die Verwendung gefälschter Meldezettel festzustellen. Durch diesen wird ein inländischer Wohnsitz vorgetäuscht, der erforderlich ist, um ein Konto in Österreich zu eröffnen.

# Betrugsbekämpfung, Steuer, Zoll und Geldwäscherei

## Betrug und Schmuggel im Zollbereich

### Allgemeine Informationen

In der Praxis ergeben sich drei Hauptgruppen an Vortaten zur Geldwäscherei, nämlich Unterfakturierung, Überfakturierung und Schmuggel.

Bei **Überfakturierung** handelt sich um eine Bezahlung über den wahren Warenwert, um dadurch Geld für Korruption oder Untreue und folglich Schwarzgeld zu generieren.

**Unterfakturierung** der Importware im Zollbereich tritt insbesondere im Zollverfahren Code 42xx auf. Bei diesen werden im Mitgliedstaat, der die Verzollung durchführt, die Zollabgaben eingehoben. Anschließend an die Verzollung erfolgt eine innergemeinschaftliche Lieferung ins Bestimmungsland, wo die Einfuhrumsatzsteuer abgeführt werden sollte.

**Schmuggel** findet besonders im Bereich von Verbrauchsteuern bei Zigaretten, Mineralölprodukten, bei gefälschten Medikamenten und Drogen statt.

### Bedrohung

Bedrohungen bestehen durch die drei genannten Delikte.

#### Überfakturierung

Generierung von Gelder im Zusammenhang mit einer Vortat z.B. Korruption oder Untreue, die dann im Rahmen der Geldwäsche in den Verkehr gebracht werden.

#### Unterfakturierung

Bedrohung besteht beim Betrug im Verfahren mit Code 42xx. Dieses Zollverfahren bietet für redliche Wirtschaftsbeteiligte den Vorteil, dass die Einfuhrumsatzsteuer zum Zeitpunkt der Verzollung nicht eingehoben wird. Andererseits birgt dieses Zollverfahren für die Zollverwaltungen und die Steuerverwaltungen in den Mitgliedstaaten (MS) der Europäischen Union hohe Risiken. Es werden beispielweise im Importland bei den Verzollungen unterfakturierte Rechnungen vorgelegt, welche teilweise nur 10 % des tatsächlichen Warenwertes ausweisen. Es wurden auch bei zahlreichen Kontrollen Mehrmengen im Vergleich zu den Angaben in den Frachtpapieren festgestellt. Dadurch kommt es in Österreich und europaweit zu massiven Verkürzungen bei den Zollabgaben. Zudem wird in vielen Fällen die Umsatzsteuer im Bestimmungsland nicht abgeführt, die Fakturenempfänger sind oft nicht existent (sogenannte „Missing Trader“) und die Waren werden zum Teil in andere Länder umgeleitet. Die Waren landen teilweise auf europäischen Schwarzmärkten oder gelangen in den legalen Handel, nachdem sie durch die besagte Betrugsmethode entsprechend verbilligt wurden. Ausweichszenarien über andere Mitgliedstaaten wurden ebenfalls beobachtet.

### **Schmuggel**

Durch die hohe Verbrauchsteuerlast handelt es sich um eine besonders lukrative Vortat. Im Jahr 2019 wurden in 2.062 Fällen insgesamt 4,989.552 Stück Zigaretten und 5,9 Tonnen anderer Rauchtobak beschlagnahmt.

#### **Conclusio:**

**Zusammenfassend ist die Bedrohung als mittel einzustufen.**

### **Verletzbarkeit**

#### **(a) Risikopotential:**

Hohe Volumina an Warenbewegungen über Drittlandsgrenzen sowie die Involvierung zahlreicher öffentlicher und privater Beteiligter erschweren die Transparenz und Nachverfolgung.

#### **(b) Risikobewusstsein:**

Es besteht ein hohes Risikobewusstsein im öffentlichen und privaten Bereich.

#### **(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Alle der drei genannten Sachverhalte werden durch das Finanzstrafgesetz unter Strafe gestellt. Im Bereich des Schmuggels werden stichprobenartig Kontrollen durchgeführt.

Die Zollbehörde verfügt über eine Risikoanalyse und darauf aufbauende IT-Systeme, die jeder Warenkategorie eine eigene Risikostufe zuweisen und die Frequenz der Überprüfungen durch Zöllner steuern.

#### **Human- und Finanzressourcen:**

Gesamt stehen 271,6 Vollbeschäftigtenäquivalente zur Verfügung, die sich auf die Fachabteilung Betrugsbekämpfung, Weiterbildung und Zollämter aufteilen.

#### **Conclusio:**

**Zusammenfassend ist die Verletzbarkeit als mittel einzustufen.**

### **Risikomindernde Maßnahmen**

Die Zollverwaltung führt laufende Identifizierung von Betrugsszenarien und Beteiligten durch. Zusätzlich findet Prävention durch Guidelines an die Mitarbeiter sowie Schulungen statt. Die EU-Kommission hat gemeinsam mit den MS europaweit geltende Indikatoren und Kriterien zur Identifizierung von Unterfakturierung erarbeitet, die von den MS angewandt werden. Es erfolgte eine Profilerstellung bei Verzollung und nachträglicher Kontrolle beim Empfänger-Spediteur.

### **Gesamtrisiko**

**Im Bereich der drei Sachverhalte besteht ein mittleres Risiko.**

### **Empfehlungen**

Wenn ein Mitgliedstaat erfolgreiche Maßnahmen ergreift, weichen die Akteure sofort in den nächsten Mitgliedstaat aus. Das Problem kann nur EU-weit gelöst werden.

## Steuervortaten

### Allgemeine Informationen

Finanzvergehen als Vortaten der Geldwäscherei (§ 165 StGB):

- Abgabenhinterziehung nach § 33 FinStrG mit einem strafbestimmenden Wertbetrag > 100.000 EUR
- Schmuggel nach § 35 FinStrG mit einem strafbestimmenden Wertbetrag > 50.000 EUR
- Hinterziehung von Eingangs- oder Ausgangsabgaben nach § 35 FinStrG mit einem strafbestimmenden Wertbetrag > 50.000 EUR
- Vorsätzliche Abgabenhilerei nach § 37 FinStrG mit einem strafbestimmenden Wertbetrag > 50.000 EUR
- Grenzüberschreitender Umsatzsteuerbetrug nach § 40 FinStrG

### Bedrohung

Nachstehend wird eine demonstrative Liste von Bedrohungsszenarien für die obgenannten Vortaten angeführt. Im Schnitt wurden im letzten Jahrzehnt um die 150 Schuldsprüche pro Jahr vom Gericht verhängt.

#### Bedrohungsszenarien

- Der Kunde / Klient erhält Geldbeträge und die Unterlagen (Rechnung) kommen aus einem Offshore-Sanktions-Land
- Der Kunde/ Klient ist Sozialhilfeempfänger oder hat nur geringes offizielles Einkommen, erhält aber regelmäßig Überweisungen von anderen Konten, ev. unter Angabe einer Rechnungsnummer
- Der Kunde/ Klient überweist regelmäßig Beträge an bekannte Krypto-Tauschbörsen bzw. erhält Beträge von diesen, die Unterlagen (Rechnung) kommen aus einem Offshore-Sanktions-Land
- Der Kunde / Klient ist als Scheinunternehmer auf der Liste der Scheinunternehmer angeführt
- Ein großer Teil der Transaktionen wird bar abgewickelt

Oftmals treten diese Szenarien in Kombination auf. Die größten Bedrohungen bestehen grundsätzlich bei Sachverhalten mit Offshorebezug.

Aus den Verurteilungszahlen ist zu erkennen, dass finanzstrafrechtliche Vortaten eine konstante Bedrohung darstellen.

#### Conclusio:

**Zusammenfassend ist die Bedrohung als mittel einzustufen.**

### Verletzbarkeit

#### **(a) Risikopotential:**

Da es sich um eine Analyse der Vortaten handelt, entfällt die Einschätzung eines Risikopotentials.

#### **(b) Risikobewusstsein:**

Im Bereich der Steuerverwaltung ist sehr gutes Risikobewusstsein vorhanden.

Im Finanzsektor ist das Risikobewusstsein grundsätzlich gut, während es im Nichtfinanzsektor unterschiedlich ausgeprägt ist.



**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Der rechtliche Rahmen ist durch die Steuergesetzgebung umfassend geregelt.

**Human- und Finanzressourcen:**

Gesamt stehen 8 Vollbeschäftigtenäquivalente zur Verfügung, die sich auf die Fachabteilung Betrugsbekämpfung, Abteilung für Risikomanagement (PACC) und das Amt für Betrugsbekämpfung aufteilen und für die Bearbeitung der Geldwäsche-Verdachtsmeldungen zuständig sind.

Auch ist darauf hinzuweisen, dass alle Mitarbeiter des Finanzamtes Österreich und der Großbetriebsprüfung bei Hinweisen auf Vortaten die zuständigen Stellen verständigen.

**Conclusio:**

**Zusammenfassend liegt eine mittlere Verletzbarkeit vor.**

**Risikomindernde Maßnahmen**

Schulungen finden im öffentlichen und privaten Sektor statt. Die Abteilung für Risikomanagement (PACC) führt laufend Risikoanalysen hinsichtlich der Vortaten durch.

**Gesamtrisiko**

**Zusammenfassend ist das Risiko als mittel einzustufen.**

**Empfehlungen**

Weiterführung der Schulungen und Fortbildungsmaßnahmen sowie der Durchführungen von Risikoanalysen.

**Betrug in Verbindung mit Offshore****Allgemeine Informationen**

Der Begriff „Offshore“ umfasst einerseits klassische Steueroasen, andererseits Rechtsordnungen, die niedrige Steuerbelastung (15 % oder weniger direkte Steuer) oder Steuerbegünstigungen (grundsätzlich oder zeitlich befristet) systematisch zulassen. Sie ermöglichen dem Kunden zusätzlich ein hohes Maß an Anonymität.

Offshore-Konstruktionen dienen folgenden Zwecken:

- Keine oder niedrige Steuern in den betreffenden Destinationen verbunden mit einem hohen Maß an Vertraulichkeit durch striktes Bankgeheimnis sowie Geheimhaltung hinsichtlich der Identität des wirtschaftlichen Eigentümers sowie der Transaktionen und die Unmöglichkeit des Informationsaustausches mangels Amtshilfe-Rechtshilfeabkommen.
- Sofern Abkommen abgeschlossen wurden, werden keine inhaltlichen Informationen übermittelt, da eine wirtschaftliche Aktivität im jeweiligen Territorium untersagt wird.

**Bedrohung**

Offshore-Konstruktionen sind ein wesentlicher Indikator für Geldwäsche. Durch OFFSHORE-Leaks (z.B. PANAMA-Papers, LUX-Leaks etc.) wurden eine Vielzahl an Straftaten, die durch Offshore-Jurisdiktionen ermöglicht wurden, bekannt. Offshore-Konstruktionsformen wer-

den nicht nur zur Steuerhinterziehung, sondern auch zur Begehung einer Vielzahl strafrechtlicher Delikte, wie etwa Betrug, betrügerische Krida, Untreue, aber auch für Amtsdelikte (Korruption/Bestechungen) verwendet.

In Österreich wurden folgende Bedrohungsszenarien beobachtet:

**Fallstudie 1:**

Ein Offshore-Unternehmen eröffnet ein Konto im Inland. Auf dieses Konto gehen Auslandszahlungseingänge von tatsächlich tätigen Unternehmen und Offshore-Unternehmen ein. Die angesammelten Kontoguthaben werden bar behoben bzw. weiterüberwiesen. Es gibt kaum inländische Ermittlungsansätze, da das Grundgeschäft nicht in Österreich abgewickelt wird. Weiters ist kaum feststellbar, wer der tatsächlich wirtschaftlich Berechtigte der Unternehmung ist. Ausländische Staatsangehörige sind bevollmächtigt. Es liegt die Annahme nahe, dass über solche Konstruktionen Geldwäscherei betrieben wird.

**Fallstudie 2:**

Ein Offshore-Unternehmen besitzt eine inländische Geschäftsadresse und/oder ein Konto im Inland. Von der inländischen Geschäftsadresse werden administrative Tätigkeiten – „Postsendungen“, „Rechnungslegungen“, „Telefonumleitungen“, „Zahlungsanweisungen“, etc. – durchgeführt. Kriminalpolizeilich bestehen kaum inländische Ermittlungsansätze, da das Grundgeschäft nicht in Österreich abgewickelt wird und unbekannt ist, wer tatsächlich wirtschaftlich Berechtigter ist. Es ergeben sich enorme Kontoumsätze, die Informationen – vorausgesetzt sie liegen vor – sind nicht aussagekräftig und ermöglichen keine Einleitung von kriminalpolizeilichen Ermittlungen. Es liegt die Annahme nahe, dass über solche Konstruktionen Geldwäscherei betrieben wird.

**Fallstudie 3:**

Eine österreichische juristische Person ist Tochter eines ausländischen Offshore-Unternehmens. Sie wurde von einem ausländischen Treuhänder gegründet und kann sowohl von Österreich als auch vom Ausland verwaltet werden. Falls Warenlieferungen erfolgen, so werden diese lediglich über Österreich – ohne Umsatzsteuer – verrechnet, die Zahlungen betreffen jedoch häufig „geistige Leistungen“ wie „feasibility studies“, „consultancy agreements“, etc. Es ergeben sich enorme Kontoumsätze. Österreichische Staatsangehörige treten als Geschäftsführer, Vorstand bzw. Gesellschafter auf. Die juristischen Personen haben idente Firmenadressen. Diese stellen Scheinrechnungen für fiktive Grundgeschäfte aus. Es liegt die Annahme nahe, dass über solche Konstruktionen Geldwäscherei betrieben wird.

**Conclusio:**

**Zusammenfassend ist die Bedrohung als sehr hoch einzustufen.**

**Verletzbarkeit**

**(a) Risikopotential:**

Das Rechtssystem und die Behörden gewähren ausländischen Kunden niedrige Steuern verbunden mit einem hohen Maß an Vertraulichkeit durch Bankgeheimnis sowie Geheimhaltung. Zudem besteht hinsichtlich der Transaktionen die Unmöglichkeit des Informationsaustausches mangels Amtshilfe-Rechtshilfeabkommen.

Die Österreichische Steuerverwaltung hatte 2019 211 Ersuchen an Offshore-Destinationen gestellt. Es erfolgt selten eine Antwort.

**(b) Risikobewusstsein:**

Sowohl bei Behörden als auch im Privatsektor besteht hohes Risikobewusstsein für Konstruktionen in Zusammenhang mit Offshore-Jurisdiktionen.

**(c) Rechtlichen Rahmenbedingungen und Aufsicht/Governance:**

Die folgenden Rechtsakte sollen Anonymität bei wirtschaftlichen Transaktionen mit Auslandsbezug mindern und den Informationsaustausch fördern:

Automatischer Informationsaustausch über Finanzkonten nach § 91 GMSG (DAC 2-CRS), EU-Meldepflichtgesetz (EU-MPFG), Doppelbesteuerungsabkommen (AHE), Delegierte Verordnung der Europäischen Kommission (2016/1675) gem. Art. 9 Abs. 2 der RI (EU) 2015/849 in der geltenden Fassung.

**Human- und Finanzressourcen:**

In der Abteilung für Betrugsbekämpfung ist ein Vollbeschäftigtenäquivalent vorgesehen. Im Zuge der Tätigkeiten der Steuerverwaltung stellt das Amt für Betrugsbekämpfung laufend Ersuchen an Offshore-Destinationen.

**Conclusio:**

**Zusammenfassend ist die Verletzbarkeit als sehr hoch einzustufen.**

**Risikomindernde Maßnahmen**

Neben dem bereits angeführten rechtlichen Rahmen bestehen die folgenden risikomindernden Maßnahmen:

- Schulungen von Verpflichteten, regelmäßige Zusammenarbeit zwischen zuständigen Behörden und Verpflichteten, BEPS (Base Erosion and Profit Shifting) Maßnahmen.
- Stärkung der Mitwirkungspflicht bei Auslandssachverhalten im Bereich des Abgabenverfahrens (vgl. § 115 Abs. 1 Bundesabgabenordnung (BAO)), Behandlung im FMA-Rundschreiben zu Sorgfaltspflichten.
- Das Kontenregister stellt den Behörden wichtige Informationen bei der Prävention und Bekämpfung zu GW/TF zur Verfügung.

**Gesamtrisiko**

**Zusammenfassend ist das Risiko als sehr hoch einzustufen.**

**Empfehlungen**

Der internationale Informationsaustausch sollte durch internationale Abkommen ermöglicht und gestärkt werden.

**Virtuelle Währungen und Kryptoassets**

**Allgemeine Informationen**

Virtuelle Währungen sind durch § 2 Z 21 FM-GwG legaldefiniert.

**Bedrohung**

In den zusammengefassten Szenarien der SNRA wurde die Bedrohung, dass virtuelle Währungen für Geldwäscherei missbraucht werden, mit einem hohen Risiko eingestuft. In der Folge soll die nationale Bedrohung abgeleitet werden.

Auf Grund der derzeit eingeschränkten Regulierung und Aufsicht im Kryptobereich weichen Kriminelle zunehmend auf diese Zahlungsmethoden aus. Durch die rasante Steigerung der Beliebtheit kommt es zudem zur Begehung von Vortaten, die mit Kryptoassets in Zusammenhang stehen. Dazu zählt insbesondere die Verbreitung von Ransomware, die Lösegeldzahlung in Kryptowährung fordert. Im Darknet stellen Kryptowährungen die einzige Zahlungsmöglichkeit dar.

Im Bereich der Geldwäsche werden Kryptowährungen zur Verschleierung genutzt.

**Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine hohe Bedrohung nahelegen, zeigen die aktuellen nationalen Daten, dass eine sehr hohe Bedrohung besteht.**

**Verletzbarkeit**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von virtuellen Währungen im Hinblick auf den Missbrauch für die Zwecke der Geldwäscherei hoch/sehr hoch eingestuft.

**(a) Risikopotential:**

Die Anonymität erschwert den Zugang zu Informationen über Finanzströme und Benutzerdaten und somit die Ermittlungen. Diese unterscheidet sich je nach Art und technischer Ausgestaltung der Kryptowährung. Schwierigkeit der Behörden den Zugangscode zu einer Wallet, die potentielle illegale Vermögensbestandteile enthält, sicherzustellen. Die Ermittlungen im Vollzugsbereich sowie die Sicherstellung von Vermögenswerten und Exekution werden dadurch erschwert. Auch die Nachvollziehbarkeit von Finanzströmen ist im Vergleich zum regulierten Fiat-Finanzsektor wesentlich schwächer.

**(b) Risikobewusstsein:**

Sowohl der öffentliche Sektor als auch der Privatsektor weisen ein hohes Risikobewusstsein auf.

**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Durch eine Novelle des FM-GwG sind nunmehr auch Anbieter in Bezug auf virtuelle Währungen verpflichtet. Sie sind damit den Sorgfaltspflichten des FM-GwG unterworfen, müssen sich bei der FMA registrieren und werden durch diese beaufsichtigt.

**Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine hohe/sehr hohe Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von virtuellen Währungen, für die Zwecke der Geldwäscherei missbraucht zu werden, als hoch einzustufen ist.**

**Risikomindernde Maßnahmen**

Das BMF beteiligt sich an Forschungsprojekten mit anderen Behörden, dem Privatsektor und der Wissenschaft. Die Forschungsprojekte fließen auch in die Schulung der Mitarbeiter ein. In der Abteilung für Betrugsbekämpfung ist ein Vollbeschäftigungsäquivalent zugewiesen. Das Projektvolumen der Forschungsprojekte beträgt 1,6 Mio Euro über vier Jahre.

**Gesamtrisiko**

**Das Gesamtrisiko ist als sehr hoch einzustufen.**

### Empfehlungen

Der internationale Austausch von Bankinformationen für Steuerzwecke sollte auf den Kryptobereich ausgedehnt werden. Die Fortsetzung der Forschungsprojekte soll den Behörden ein umfassendes Verständnis des Sektors ermöglichen.

### ANNEX. Das Kontenregister als Maßnahme zur Bekämpfung von Betrug und Geldwäscherei

#### Allgemeine Informationen

Das Kontenregister stellt den Behörden wichtige Informationen bei der Prävention und Bekämpfung zu GW/TF zur Verfügung. Die Datenqualität wird durch automatisierte Verfahren und Kontrollen erhöht. Abfrageberechtigt sind Staatsanwaltschaften, Strafgerichte, Abgabenbehörden des Bundes, Finanzstrafbehörden, das Bundesfinanzgericht, die FIU, BVT, BK, BAK, FMA und OeNB.

#### Empfehlungen

Es ergeben sich Lücken durch die mangelnde Erfassung von Kreditkonten und den eingeschränkten Anwendungsbereich bei Anbietern, die Schließfachdienste nicht als Haupttätigkeit anbieten.

Eine Verbesserung der verfügbaren Informationen würde sich durch die Erfassung der Kontostände ergeben.

# Bedrohungsszenarien der Terrorismusfinanzierung

Risiko der Terrorismusfinanzierung
<b>Allgemeine Informationen</b>
Wer <b>Vermögenswerte</b> mit dem Vorsatz bereitstellt oder sammelt, dass sie, wenn auch nur zum Teil der Ausführung ... von terroristischen Straftaten ... verwendet werden (§ 278d StGB). <b>Vermögenswerte</b> sind materielle, immaterielle, bewegliche oder unbewegliche Gegenstände, egal wie sie erworben wurden, rechtserhebliche Schriftstücke oder Urkunden (elektronisch/digital), die das Recht auf Vermögensgegenstände oder Rechte daran belegen, Bankkredite, Reiseschecks, Bankschecks, Zahlungsanweisungen, Aktien, Wertpapiere, Schuldverschreibungen, Wechsel, Akkreditive etc.
<b>Bedrohung</b>
<p>Die Finanzierung des Terrorismus beschränkt sich derzeit vorrangig auf die Erhaltung der Organisation terroristischer Gruppierungen. Die Führung einer solchen, auch wenn sie sich nicht in einem Krisengebiet befindet, benötigt finanzielle Ressourcen für strategische Aufgaben, wie z.B. Propaganda, Rekrutierung neuer Mitglieder und für das Bestreiten der Organisationskosten bzw. Lebenserhaltungskosten der Kader. Verglichen mit den 70er und 80er Jahren, wo Österreich noch Zielland terroristischer Attacken war, ist es zu einem Transit- und Rückzugsland geworden, wo Finanzierung, Rekrutierung und Propaganda betrieben wird.</p> <p>Im Jahr 2020 leben in Österreich 707.780 (2015: 566.000) Drittstaatsangehörige, von welchen etwa 42 % vom Westbalkan stammen. Zirka 16 % sind türkische Staatsbürger. Aus den Staaten des sogenannten „Arabischen Frühlings“ stammen mittlerweile 96.425 Personen (oder 13,6 %). Aus der Krisenregion Afghanistan/Pakistan kommen 47.766 Personen (oder 6,7%). 32.872 Personen (oder 4,6 %) besitzen die Staatsbürgerschaft der Russischen Föderation, von denen ein großer Teil aus dem Nordkaukasus stammt. All diese Gegenden sind oder waren in jüngster Vergangenheit Konfliktregionen (Türkei, Nordkaukasus, Ex-Jugoslawien, Afghanistan, Irak, Syrien).</p> <p>Daneben gab es seit ca. 15 Jahren den Trend zu Dschihadreisen von österreichischen Konvertiten oder hier lebenden Drittstaatsangehörigen, zuerst nach Afghanistan und seit 2013 nach Syrien und in den Irak, was ein neueres Phänomen darstellt, da diese Konvertiten im Inland keiner terroristischen Gruppierung angehörten, sondern sich dort den verschiedenen Gruppierungen in den Krisenregionen anschlossen. Die Personenzahl, die nach Syrien und in den Irak ausreiste oder versuchte dorthin auszureisen, war nicht gering. Nach Zerschlagung des IS ist dieser Trend mittlerweile stark rückläufig. Derzeit sind Angehörige und Freunde dieser Dschihadreisenden darauf aus, ihre Verwandten bzw. Freunde bei der Rückkehr zu unterstützen bzw. sie aus der Gefangenschaft freizubekommen. Mittlerweile geht von Rückkehrern aus dem Dschihad ein unbestimmtes Gefahrenpotential aus, denn manche sind geläutert, andere wiederum halten an ihren radikalen Ideen fest.</p>

**Mittelaufbringung – Spenden:**

Terrororganisationen sammeln vorwiegend in der eigenen Community Gelder ein und gehen hierbei sehr klandestin vor. Je mehr sich die Spender mit der „Sache“ der Organisation identifizieren können, desto leichter ist es Gelder zu lukrieren. Oftmals verfügen Sympathisanten terroristischer Organisationen nur über sehr beschränkte finanzielle Ressourcen. Dennoch ist bekannt, dass durch Spendensammlungen mitunter ansehnliche Beträge erzielt werden können. Das Einsammeln der Gelder erfolgt durch Mittelsleute oder über nicht reglementierte Crowdfundingformen. Im Jahr 2012 konnte durch unregelmäßige Crowdfundingformen von einem Zwei-Personen-Verein in kurzer Zeit der Betrag von € 22.000,- gesammelt werden, wobei das offizielle Ziel der Sammlung einem humanitären Zweck im Ausland diente. Der wahre Zweck ist den vielen Kleinspendern (meist) gar nicht bekannt. Außerdem ist das Geben einer Spende in vielen Religionen ein Gebot und besteht meist aus Klein- und Kleinstbeträgen. Bei gut organisierten Gruppierungen werden (Kultur-)Vereine zur Abdeckung des wahren Zwecks betrieben, wobei nach außen hin der kulturelle Zweck des Vereins in den Vordergrund gestellt wird.

**Überweisungen in Drittstaaten:**

TEFIN-Gelder sind fast ausschließlich für Drittstaaten bestimmt (Russische Föderation, Türkei, Naher Osten, Somalia, Afghanistan, Pakistan, Irak, Syrien, etc.), sodass das letzte Empfängerland und der End-Empfänger kaum verlässlich ermittelt werden kann, da Gelder mitunter auch über andere Drittstaaten weitergeleitet werden.

Darüber hinaus gibt es Erkenntnisse zu Überweisungen von Angehörigen oder aus dem engen Umfeld von in Krisengebiete gereiste Personen, welche sich dem bewaffneten Dschihad anschließen möchten oder bereits angeschlossen haben, sowie jenen, welche sich erst auf der Reise in diese Regionen befinden.

Nach wie vor ist die Türkei aufgrund ihrer geographischen Lage eine von terroristischen Gruppierungen sowie deren Sympathisanten für Finanztransaktionen oft genutztes Drittland, wenn Dschihadreisende mit Geldern versorgt werden sollen.

Weiters sind in der Türkei gegen diesen Staat gerichtet Terrororganisationen aktiv, womit die Türkei auch als Zielland von Transaktionen zu sehen ist.

Gelder werden einerseits von offiziellen Finanzdienstleistern (MVTs) und, sollte dies nicht opportun bzw. möglich sein, z.B. wenn es dorthin keine Bankverbindung gibt, von Inoffiziellen (Hawaladare) in das Zielland übermittelt. Es können beliebig viele Mittels-/Strohleute dazwischengeschaltet werden, um die Enddestination zu verschleiern. Terrororganisationen nutzen generell Bargeldkuriere, wenn größere Summen zu transferieren sind, um somit den strikten Auflagen hinsichtlich Geldwäsche und Terrorismusfinanzierung, denen die Verpflichteten (obligated entities) unterliegen, zu entgehen.

Andererseits erfolgen Überweisungen über einen Drittstaat oder durch eine in einem anderen Staat gelegenen Korrespondenzbank, wenn es zum Zielland keine direkte Bankverbindung gibt. Diese Geldtransfer-Umschlagplätze werden aber von vielen Personen aus den unterschiedlichsten Beweggründen genutzt (familiäre Unterstützung im Heimatland, Handel ...).

Daher kann es zu keiner Generalverdächtigung hinsichtlich dieser Überweisungen kommen, da Mittelsleute neben dem Argument der fehlenden Infrastruktur in der Krisenregion vorwiegend aus persönlichen Gründen in Anspruch genommen werden. Denn abgesehen von den legalen Finanzdienstleistern wie Banken und Remittance-Dienstleistern (Western Union, MoneyGram, Coinstar, etc.) werden oftmals, obgleich dies aufgrund der übernom-

menen Treuhandenschaft rechtlich im Regelfall nicht zulässig ist, vertrauenswürdige Kontaktpersonen im Ausgangsland bzw. Empfangsland mit der Transaktion betraut. Bei solchen Vertrauenspersonen handelt es sich zumeist um Ko-Nationale oder zumindest um Personen aus demselben Kulturkreis.

Bargeldkuriere können nur vom Zoll beim Betreten und Verlassen des EU-Gebietes erfasst werden, was aber im Bundesgebiet nur mehr auf Flughäfen und an der Grenze zur Schweiz und Liechtenstein möglich ist (§ 17b ZollR-DG).

**Verdachtsmeldungen:**

Wie aus der Position „Fälle bei StA“ ersichtlich ist, führen nur wenige der von österreichischen Finanzdienstleistern wegen des Verdachts auf Terrorismusfinanzierung bei der A-FIU eingebrachten Verdachtsmeldungen zu einer tatsächlichen strafprozessualen Verfolgung und noch geringer sind die dadurch erzielten Verurteilungen.

Jahr	2015	2016	2017	2018	2019	2020
Verdachtsmeldung	113	148	203	167	93	113
Fälle bei Staatsanwaltschaft	46	50	54	19	20	3
Verurteilung	0	0	1	3	2	4

Anmerkung 1: Es wurden nur die Verdachtsmeldungen hinsichtlich Terrorismusfinanzierung gezählt. Es gibt aber noch VM von/nach bestimmten Destinationen, die ebenfalls überprüft werden.

Anmerkung 2 zu 2015: Eigentlich *eine* Verurteilung, da eine Person wegen § 278b verurteilt wurde, der als Teil einer terr. Organisation Gelder im großen Maße gesammelt hat.

Bei der überwiegenden Anzahl der Fälle wird ein auffälliges Kundenverhalten sowie die Übereinstimmung des Namens bzw. von Namensteilen des Auftraggebers oder Empfängers mit auf Sanktionslisten (EU, VN, OFAC, ...) befindlichen Namen von Personen oder Organisationen, von den die Verdachtsmeldungen erstattenden Finanzdienstleistern als (Haupt-)grund genannt. Des Weiteren werden die Höhe der Transaktionssummen und die Häufigkeit der vorgenommenen Transaktionen als auffällig benannt.

Die Qualität der Verdachtsmeldungen hat sich zunehmend verbessert. Dies ist vermutlich auf die eingelebte Routine bei den Meldepflichtigen zu zurückzuführen. Es gibt hierbei aber auch immer wieder Schwankungen.

Wichtig ist, dass Verpflichtete neben der Überprüfung objektiver Kriterien, wie Namensgleichheiten, Sanktionslisten oder bestimmten Destinationen immer alle Umstände abwägen (Know your customer). Personen und Organisationen, die zum Zwecke der Terrorismusfinanzierung die Leistungen eines Finanzdienstleisters in Anspruch nehmen, sind sich bewusst, dass ihre Handlungen einer Kontrolle unterzogen werden, weshalb grundsätzlich von einer (versuchten) Verschleierung der tatsächlichen Mittelverwendung auszugehen ist, etwa durch Vortäuschung eines nicht realen Spendengrundes.



Eine tatsächliche Beobachtung des Kundenverhaltens wird allerdings angesichts der sich ändernden Bankenpolitik - weg vom Schalter, hin zu „Online-Geschäften“ - immer schwieriger. Tatsächlich ist bereits jetzt die Effektivität des österreichischen „Know your customer – Systems“ zu hinterfragen (Stichwort: Online-Registrierung).

Sobald ein Gelddienstleister zum De-risking übergeht und das Kundenkonto sperrt, so dass der Betroffene in weiterer Folge schließlich keine Bank mehr findet, die bereit ist, ein Konto zu eröffnen oder Überweisungen zu tätigen, verschwindet diese Person komplett aus den Augen der Verpflichteten und indirekt aus denen der Aufsichts- und Polizeibehörden, da sie Transaktionen entweder im informellen Geldtransfernetz (Hawala) oder durch Strohleute durchführen lässt oder auf alternative Zahlungsmittel wie Bitcoin umsteigt.

Letztlich ist zu festzuhalten, dass es fast nicht möglich ist, den Endzweck von Geldüberweisungen in das Ausland zu ermitteln, um somit feststellen zu können, ob die jeweilige Geldsendung einen terroristischen Zweck hatte.

**In Österreich relevante Risiken:**

In Österreich werden legale Quellen der Finanzierung bzw. der Mittelaufwendung für terroristische Organisationen und Einzelpersonen wie z.B. durch Spenden(sammlungen), Arbeitseinkommen, Sozialhilfe, aber auch Kredite u.a. genutzt. Geldbeschaffung durch kriminelle Taten (Raub, Diebstahl, Betrug etc.) wurden bis dato nicht festgestellt. Die Mittelaufbringung für Kleingruppen bzw. Einzelpersonen, die am Dschihad in Syrien/Irak teilgenommen haben bzw. dies versuchten, wird im Regelfall aus eigenen Mitteln und vom Familien- und Freundeskreis bestritten.

# Risiken der Proliferationsfinanzierung

<b>Risiko der Proliferation</b>
<b>Allgemeine Informationen</b>
<p>Das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung und die 9 Landesämter für Verfassungsschutz und Terrorismusbekämpfung sind die verantwortlichen Stellen bei polizeilichen Ermittlungen in Bezug auf Proliferationsaktivitäten oder Sanktionsbrüche.</p> <p>Im Bereich der Exportkontrolle unterliegen Waffen, militärische Güter und Dual-Use-Güter einer Genehmigungspflicht. Das BVT ist in die Entscheidungsprozesse im Rahmen der Exportkontrolle eingebunden und leistet dadurch einen wichtigen Beitrag zur Verhinderung von illegalen Gütertransfers.</p> <p>Darüber hinaus koordiniert das BVT die interministerielle Zusammenarbeit bei den nationalen Bemühungen zur Proliferationsbekämpfung: Bei behördenübergreifenden Sitzungen werden aktuelle nationale und internationale Entwicklungen diskutiert und gemeinsame Maßnahmen und deren Auswirkungen erörtert.</p>
<b>Bedrohung</b>
<p>Die Bekämpfung der Proliferation wird auch weiterhin zu den zentralen Sicherheitsaufgaben Österreichs zählen. Die Gefahr, dass Massenvernichtungswaffen, Trägersysteme, Dual-Use Güter und entsprechendes Know-How in den Besitz sanktionierter Regime oder terroristischer Organisationen gelangen oder bestimmte Güter entgegen offizieller Angaben für eine proliferationsrelevante Verwendung missbräuchlich herangezogen werden, stellt eine der wesentlichen proliferationsbezogenen Gefährdungen dar.</p> <p>Österreich ist in diesem Zusammenhang nicht nur Transitstaat proliferationsrelevanter Güter, sondern aufgrund seiner hochentwickelten industriellen Produktion sowie der Vielzahl an klein- und mittelständischen Unternehmen, die in Teilbereich weltweit führend sind, auch Zielland für illegale Beschaffungsaktivitäten. Eine besondere Problematik stellen dabei Dual Use Güter dar, also Materialien oder Produkte, die aufgrund ihres hohen Entwicklungsstandes sowohl im zivilen als auch im militärischen Bereich Verwendung finden können.</p> <p>Eng verbunden mit dem Phänomen der Proliferation ist das Phänomen der Geldwäsche. Die Zahl der Meldungen aus dem Bankensektor zeigt, dass das Bewusstsein und die Sensibilität der österreichischen Finanzdienstleister zu den angeführten Herausforderungen deutlich zugenommen haben.</p> <p>Diese erhöhte Sensibilität trifft auch auf die Umsetzung internationaler Sanktionen in Zusammenhang mit Non-Proliferation zu.</p> <p>Sämtliche Analyseberichte betreffend Geldwäsche weisen darauf hin, dass sowohl die Komplexität als auch die Kreativität der Verschleierungsmethoden zunehmen. Diese Tatsache zeigt, dass weiterhin das Bewusstsein für die Gefahren illegaler Finanzierungen und Geldmittel gesamt gestärkt werden muss, um den Bedrohungen entgegentreten zu können.</p>

In Anbetracht der Vielzahl an internationalen oder innerstaatlichen Konflikten und des Missbrauchs von Waffen jeglicher Art durch substaatliche Gruppierungen, die in den Besitz chemischer, biologischer, radioaktiver oder nuklearer Stoffe gelangen könnten, erhöht sich der Risikofaktor für den Bereich der Proliferation erheblich.

#### **Risikomindernde Maßnahmen**

Im Rahmen eines nationalen Awareness-Programms zur Bewusstseinsbildung, einer Initiative zur exportspezifischen Sensibilisierung der österreichischen Wirtschaft, werden zudem eine Vielzahl an Unternehmen über aktuelle Problemstellungen durch das BVT informiert, um die Involvierung hiesiger Firmen in illegale Beschaffungsvorgänge frühzeitig aufzuklären und zu verhindern.

# Risiko juristischer Personen und Trusts

Für die Zwecke von Geldwäscherei und Terrorismusfinanzierung können juristische Personen und Trusts missbraucht werden, weswegen in der Folge das diesbezügliche Risiko erhoben wurde. Zu diesem Zweck hat die WiEReG-Registerbehörde eine detaillierte Analyse durchgeführt, die auch die Basis für die risikobasierte Aufsicht über das Register der wirtschaftlichen Eigentümer bildet.

<b>Juristische Personen und Trusts</b>					
<b>Allgemeine Informationen</b>					
Der Anwendungsbereich des WiEReG umfasst mit Stichtag 01.01.2021 insgesamt 366.719 Rechtsträger. Nach Rechtsformen aufgeschlüsselt sind damit folgende Rechtsträger im Register der wirtschaftlichen Eigentümer erfasst:					
	Anzahl		Anzahl		Anzahl
Personengesellschaften (OG, KG)	65.634	Versicherungsvereine und Sparkassen	80	Vereine	126.187
Aktiengesellschaften	976	Europäische Rechtsformen (EWIV, SE und SCE)	43	Gemeinnützige Stiftungen und Fonds	629
Gesellschaften mit beschränkter Haftung	168.398	Privatstiftungen	3.033	Trusts	4
Erwerbs- und Wirtschaftsgenossenschaften	1.700	Sonstige Rechtsträger	33	Trustähnliche Vereinbarungen	2

**Transparenz der wirtschaftlichen Eigentümer:**

Die oben genannten Rechtsformen sind Rechtsträger gemäß § 1 Abs. 2 WiEReG und daher dazu verpflichtet, ihre wirtschaftlichen Eigentümer an das Register der wirtschaftlichen Eigentümer zu melden. Ebenso enthält das WiEReG Informationen dazu, ob die Anteile an einem Rechtsträger im eigenen Namen oder als Treuhänder für einen Treugeber gehalten werden. Die Meldequote der meldepflichtigen Rechtsträger beträgt 96,09%, jene aller Rechtsträger beträgt 89,83%. Eine automatische Datenübernahme erfolgt bei 67,86% der Rechtsträger.

**Führung des Registers der wirtschaftlichen Eigentümer:**

Das Register der wirtschaftlichen Eigentümer wird durch die im Bundesministerium für Finanzen eingerichtete Registerbehörde geführt. Die Aufgabenbereiche der Registerbehörde umfassen die fachliche und technische Leitung, das Führen von Verwaltungsverfahren, die Analyse und Überprüfung der Meldungen, das Erstellen von Anzeigen sowie die telefonische und schriftliche Beantwortung fachlicher Anfragen. Zur Erledigung dieser Aufgaben werden derzeit insgesamt sechs Mitarbeiter (VBÄ) beschäftigt. Zwangsstrafen zur Erzwingung der Meldepflicht werden vom Finanzamt Österreich verhängt. Für die Ahndung von Meldepflichtverletzungen ist das Amt für Betrugsbekämpfung zuständig.

**Bedrohung****Geldwäscherei & Terrorismusfinanzierung:**

In den zusammengefassten Szenarien der SNRA wurde die Bedrohung, dass juristische Personen oder Rechtsvereinbarungen für terroristische Aktivitäten missbraucht werden, mit einem mittleren Risiko eingestuft. Die Bedrohung im Hinblick auf Geldwäsche wurde hingegen mit einem hohen Risiko eingestuft. In der Folge soll eine rechtsformspezifische Bedrohung abgeleitet werden. Die Berechnung erfolgt getrennt, die entsprechenden Ergebnisse werden für Geldwäsche und Terrorismusfinanzierung gemeinsam dargestellt, im Falle von Unterschieden sind diese an den betreffenden Stellen separat ausgewiesen.

**Geografische Bedrohung:**

Für die Ermittlung der geografischen Bedrohung wurde analysiert, welcher Anteil der wirtschaftlichen Eigentümer seinen Sitz im Inland, in anderen Mitgliedstaaten, in Drittländern und in für die Terrorismusfinanzierung bzw. Geldwäsche risikobehafteten Drittstaaten hat, jeweils im Vergleich zum Gesamtstand im Register. Die Einstufung der Bedrohung richtet sich dabei nach dem jeweils relevanten Wert für risikobehaftete Drittstaaten (<0,5% niedrig; <1% mittel; <1,5% hoch; >1,5% sehr hoch):

Rechtsform	Wohnsitz Wirtschaftliche Eigentümer					Staatsbürgerschaft Wirtschaftliche Eigentümer					Bedrohung TF	Bedrohung GW
	Inland	MS	DL	RL (TF)	RL (GW)	Inland	MS	DL	RL (TF)	RL (GW)		
Personengesellschaften (OG, KG)*	96,6%	2,7%	0,6%	0,01%	0,01%	82,5%	8,9%	8,6%	1,13%	0,70%	<b>hoch</b>	<b>mittel</b>
Aktiengesellschaften	79,7%	11,0%	9,3%	0,00%	0,06%	74,3%	17,7%	7,9%	0,00%	0,00%	<b>niedrig</b>	<b>niedrig</b>
Gesellschaften mit beschränkter Haftung	90,3%	6,4%	3,3%	0,02%	0,03%	85,3%	10,0%	4,7%	0,11%	0,18%	<b>niedrig</b>	<b>niedrig</b>
Erwerbs- und Wirtschaftsgenossenschaften	99,5%	0,4%	0,1%	0,00%	0,00%	99,2%	0,7%	0,1%	0,00%	0,00%	<b>niedrig</b>	<b>niedrig</b>
Versicherungsvereine und Sparkassen	100%	0,0%	0,0%	0,00%	0,00%	98,9%	1,1%	0,0%	0,00%	0,00%	<b>niedrig</b>	<b>niedrig</b>
Europäische Rechtsformen (EWIV, SE und SCE)	42,9%	46,0%	11,1%	0,00%	0,00%	51,1%	44,4%	4,4%	0,00%	0,00%	<b>niedrig</b>	<b>niedrig</b>

Privatstiftungen	90,9%	4,8%	4,3%	0,01%	0,03%	91,0%	6,0%	2,9%	0,03%	0,01%	niedrig	niedrig
Sonstige Rechtsträger	98,1%	1,9%	0,0%	0,00%	0,00%	84,6%	9,6%	5,8%	0,00%	0,00%	niedrig	niedrig
Vereine	99,2%	0,7%	0,1%	0,00%	0,00%	95,8%	2,8%	1,4%	0,22%	0,13%	niedrig	niedrig
Gemeinnützige Stiftungen und Fonds	97,0%	2,1%	0,8%	0,00%	0,00%	93,0%	5,3%	1,7%	0,04%	0,00%	niedrig	niedrig
Trusts	52,9%	47,1%	0,0%	0,00%	0,00%	23,5%	76,5%	0,0%	0,00%	0,00%	niedrig	niedrig
Trustähnliche Vereinbarungen **	0,0%	0,0%	0,0%	0,00%	0,00%	0,0%	0,0%	0,0%	0,00%	0,00%	hoch	hoch
<b>DURCHSCHNITT</b>	<b>86,1%</b>	<b>11,2%</b>	<b>2,7%</b>	<b>0,00%</b>	<b>0,01%</b>	<b>79,9%</b>	<b>16,6%</b>	<b>3,4%</b>	<b>0,14%</b>	<b>0,09%</b>		

\* Bei **Personengesellschaften** ist die geografische Bedrohung mit **hoch (TF)** bzw. **mittel (GW)** einzustufen. Die Staatsbürgerschaft der wirtschaftlichen Eigentümer ist deutlich internationaler als der Durchschnitt und der Anteil der im Hinblick auf Terrorismusfinanzierung risikobehafteten Drittländer liegt bei den Staatsbürgerschaften bei über 1%.

\*\*Bei **trustähnlichen Vereinbarungen** sind zum Zeitpunkt der Erstellung der Risikoanalyse noch keine aussagekräftigen Daten vorgelegen. Die diesbezüglichen Indikatoren wurden daher mit einem „**hohen Risiko**“ bewertet.

**Wirtschaftliche Bedrohung:**

Für die Ermittlung der wirtschaftlichen Bedrohung wurde analysiert, welcher Anteil der Rechtsformen ihre Haupttätigkeit in einem risikobehafteten Wirtschaftsbereich entfaltet (<5% niedrig; <10% mittel; <15% hoch; >15% sehr hoch). Etwaige Unterschiede zwischen Geldwäscherei und Terrorismusfinanzierung werden über die Einbeziehung der Ergebnisse der SNRA berücksichtigt:

Rechtsform	Haupttätigkeit in risikobehafteten Wirtschaftsbereichen		Bedrohung
	absolut	relativ	
Personengesellschaften (OG, KG)	14.452	22,02%	<b>sehr hoch</b>
Aktiengesellschaften	411	42,11%	<b>sehr hoch</b>
Gesellschaften mit beschränkter Haftung	50920	30,24%	<b>sehr hoch</b>
Erwerbs- und Wirtschaftsgenossenschaften	444	26,12%	<b>sehr hoch</b>
Versicherungsvereine und Sparkassen	22	27,50%	<b>sehr hoch</b>
Europäische Rechtsformen (EWIV, SE und SCE)	43	39,53%	<b>sehr hoch</b>
Privatstiftungen	2953	97,36%	<b>sehr hoch</b>
Sonstige Rechtsträger	3	9,09%	<b>mittel</b>
Vereine	239	1,68%	<b>niedrig</b>
Gemeinnützige Stiftungen und Fonds	3	0,48%	<b>niedrig</b>
Trusts*	N/A	N/A	<b>sehr hoch</b>
Trustähnliche Vereinbarungen**	N/A	N/A	<b>sehr hoch</b>
<b>DURCHSCHNITT (Mittelwert)</b>		<b>29,61%</b>	



\* Hinsichtlich des Anteils von **Trusts** mit Haupttätigkeit in risikohaften Wirtschaftsbereichen liegen mangels ÖNACE-Erfassung keine Daten vor. Aufgrund des von Trusts im Allgemeinen verfolgten Zwecks der Vermögensverwaltung sind sie im Hinblick auf die wirtschaftliche Bedrohung jedoch mit Privatstiftungen vergleichbar, weshalb die entsprechende Einstufung von Trusts analog der ausgewerteten Daten für die Privatstiftung mit **sehr hoch** erfolgt.

\*\* Bei **trustähnlichen Vereinbarungen** liegen ebenfalls keine aussagekräftigen Daten vor, da bei den zwei in Österreich registrierten trustähnlichen Vereinbarungen keine ÖNACE-Codes vergeben wurden. Es gilt hier dieselbe Annahme wie bei Trusts.

**Rechtsformspezifische Eignung:**

In der SNRA wurden bei der Ermittlung der Bedrohung vor allem die Komplexität der Gründung und das dafür erforderliche Wissen und der rechtliche und wirtschaftliche Aufwand, um die laufende Fortführung zu bewerkstelligen, herangezogen. Etwaige Unterschiede zwischen Geldwäscherei und Terrorismusfinanzierung werden (sofern nicht separat adressiert) über die Einbeziehung der Ergebnisse der SNRA berücksichtigt. Ausgehend von diesen Annahmen kann zu den jeweiligen Rechtsformen Folgendes festgehalten werden:

Rechtsform	Rechtsform-spezifische Eignung	Begründung
Personengesellschaften (OG, KG)	<b>niedrig</b>	Die unmittelbare Involvierung der Gesellschafter, die alle aus dem öffentlich zugänglichen Firmenbuch ersichtlich sind, ist bei eingetragenen Personengesellschaften sehr stark ausgeprägt. Auch die unbeschränkte persönliche Haftung aller Gesellschafter einer offenen Gesellschaft und aller Komplementäre einer Kommanditgesellschaft sowie die schwierige Übertragbarkeit von Gesellschaftsanteilen (Ausmaß der Beteiligung aus dem Firmenbuch nicht ersichtlich, Zustimmungserfordernis aller anderen Gesellschafter) machen diese Rechtsformen für missbräuchliche Zwecke weniger attraktiv. Für kapitalistische Personengesellschaften („GmbH und Co KG“) treffen diese Aussagen zwar nur teilweise zu; dafür gelten für diese Gesellschaften zahlreiche Vorschriften des Kapitalgesellschaftsrechts (z.B. Bilanzierungspflicht).
Aktiengesellschaften	<b>niedrig</b>	Für alle wichtigen Maßnahmen der Gesellschaft ist zwingend die Mitwirkung eines Notars vorgeschrieben und durch zahlreiche Anmeldepflichten zum öffentlich zugänglichen Firmenbuch besteht insgesamt ein sehr hohes Transparenzniveau. Durch die gesetzlichen Anforderungen an die Gesellschaft und die verpflichtende Involvierung von Kreditinstituten ist auch gewährleistet, dass die Aktionäre (rechtlichen Eigentümer) stets verlässlich festgestellt werden können. Überdies ist der rechtliche und wirtschaftliche Aufwand für die laufende Fortführung hoch.
Gesellschaften mit beschränkter Haftung	<b>TF: niedrig GW: mittel</b>	Für viele wichtige Maßnahmen der Gesellschaft ist zwingend die Mitwirkung eines Notars oder eines Kreditinstituts vorgeschrieben und durch zahlreiche Anmeldepflichten zum öffentlich zugänglichen Firmenbuch besteht insgesamt ein sehr hohes Transparenzniveau. Durch die Eintragung der Gesellschafter in das öffentlich zugängliche Firmenbuch können die rechtlichen Eigentümer der Gesellschaft festgestellt werden. Da die Übertragung von Gesellschaftsanteilen trotz notwendiger Mitwirkung eines Notars bei GmbHs verhältnismäßig einfach und schnell möglich ist, führt dies im Hinblick auf Geldwäsche jedoch zu einer erhöhten rechtsformspezifischen Eignung (z.B. durch den möglichen Verkauf von „Firmenmänteln“).

Erwerbs- und Wirtschafts- genossenschaften	<b>niedrig</b>	Es handelt sich um eine sehr spezielle – und damit im geschäftlichen Verkehr von vornherein nicht „unauffällige“ – Rechtsform, die durch das gesetzliche Erfordernis der Zugehörigkeit zu einem Revisionsverband und die periodische Gebarungsprüfung durch einen vom Revisionsverband bestellten Revisor einer regelmäßigen Prüfung unterliegt. Auch der Umstand, dass Erwerbs- und Wirtschafts-genossenschaften regelmäßig eine hohe Mitgliederanzahl aufweisen, dürfte die Rechtsform für Zwecke der Geldwäsche sehr unattraktiv machen.
Versicherungsvereine und Sparkassen	<b>niedrig</b>	Die Errichtung der Rechtsträger ist mit hohen Anforderungen verbunden und aufgrund der zwingenden Eintragung im Firmenbuch sowie der umfassenden Berichts- bzw. Auskunftspflichten gegenüber der FMA besteht ein sehr hohes Transparenzniveau. Überdies ist der rechtliche und wirtschaftliche Aufwand für die laufende Fortführung aufgrund umfangreicher Governanceanforderungen hoch.
Europäische Rechtsformen (EWIV, SE und SCE)	<b>niedrig</b>	Hier ist für die EWIV auf die Einstufung für Personengesellschaften (insb. OG), für die SE auf jene für Aktiengesellschaften und für die Europäische Genossenschaft (SCE) auf die Einstufung betreffend Erwerbs- und Wirtschafts-genossenschaften zu verweisen. Durch das Erfordernis eines grenzüberschreitenden Elements bei allen drei europäischen Rechtsformen ist der Aufwand für die Gründung bzw. laufende Fortführung tendenziell noch höher als bei den jeweiligen nationalen Rechtsformen.
Privatstiftungen	<b>mittel</b>	Für viele wichtige Maßnahmen ist grundsätzlich zwingend die Mitwirkung eines Notars vorgeschrieben und durch zahlreiche Anmeldepflichten zum öffentlich zugänglichen Firmenbuch besteht insgesamt ein hohes Transparenzniveau.  Dieses wird auch durch die verpflichtende Meldung der wirtschaftlichen Eigentümer, darunter die Begünstigten, Begünstigtenkreis, Einmal- und Letztbegünstigte sowie alle Personen, die auf sonstige Weise Kontrolle ausüben, sichergestellt.  Da die Entstehung die Eintragung im Firmenbuch voraussetzt, ist zudem eine lückenlose Erfassung der Privatstiftungen im Firmenbuch und im WiReG gewährleistet. Überdies hat der Stiftungsvorstand den festgestellten Begünstigten dem für die Erhebung der Körperschaftsteuer zuständigen Finanzamt unverzüglich elektronisch mitzuteilen.
Sonstige Rechtsträger	<b>niedrig</b>	Die rechtlichen sowie finanziellen Anforderungen an die Gründung sind im Allgemeinen sehr hoch. Die strengen Governanceanforderungen sind detailliert in den jeweils zugrundeliegenden Gesetzen geregelt. Da sonstige Rechtsträger definitionsgemäß im Firmenbuch einzutragen sind und es sich bei ihnen um individuell geschaffene Einrichtungen handelt, deren Träger in der Regel Gebietskörperschaften sind, ist das Transparenzniveau sehr hoch.
Vereine	<b>TF: hoch</b> <b>GW: mittel</b>	Im Unterschied zu anderen Rechtsformen (bspw. GmbH) erfolgt keine Überprüfung der Identität der handelnden Personen und auch der rechtliche Aufwand für die Gründung und laufende Fortführung ist gering. Die Governanceanforderungen sind entsprechend der Größe eines Vereins vorgesehen und sehen ab einer Höhe der gewöhnlichen Einnahmen und Ausgaben von mehr als drei Millionen Euro eine externe Überprüfung durch einen Abschlussprüfer vor. Auf der anderen Seite ist zu berücksichtigen, dass ein Verein nur für ideelle Zwecke gegründet werden darf und nicht auf Gewinn gerichtet sein darf. Eine Bedeutung kann Vereinen allerdings im Hinblick auf die Sammlung von Spenden zukommen, die wiederum für die Zwecke der Terrorismusfinanzierung verwendet werden könnten, weshalb die rechtsformspezifische Eignung im Hinblick auf Terrorismusfinanzierung als erhöht einzustufen ist. Vereine, deren jährliches Aufkommen an im Publikum gesammelten Spenden in zwei aufeinander folgenden Rechnungsjahren jeweils den Betrag von einer Million Euro übersteigt, haben gemäß § 22 Abs. 2 VerG einen erweiterten Jahresabschluss (Bilanz, Gewinn- und Verlustrechnung, Anhang) aufzustellen und überdies für die Abschlussprüfung durch einen Abschlussprüfer zu sorgen.
Gemeinnützige Stiftungen und Fonds	<b>niedrig</b>	Es erfolgt zwar keine Überprüfung der Identität der handelnden Personen und der Aufwand für die Gründung und für die laufende Fortführung ist moderat, wenn die gewisse Größengrenzen nicht überschritten werden.  Jedoch ist risikomindernd zu berücksichtigen, dass ab einer Höhe der gewöhnlichen Einnahmen und Ausgaben von mehr als einer Millionen Euro in zwei aufeinanderfolgenden Jahren eine externe Überprüfung durch einen Stiftungs- oder Fondsprüfer sichergestellt ist und eine Bilanz, Gewinn- und Verlustrechnung und ein Lagebericht aufzustellen ist. Dadurch steigen die Kosten für die laufende Fortführung deutlich und die externen Kontrollen werden verstärkt.

		Zudem ist zu berücksichtigen, dass das Stiftungs- oder Fondsvermögen gemäß § 1 BStFG und die Erträge daraus nur zur Erfüllung gemeinnütziger oder mildtätiger Aufgaben verwendet werden dürfen.
Trusts	<b>sehr hoch</b>	Für die Errichtung eines Trusts sind weder einheitliche Formvorschriften, noch zwingende Eintragungen in öffentliche Register vorgesehen. Auch bestehen keinerlei Mitwirkungspflichten von Notaren oder Rechtsanwälten. Zudem besteht keine allgemeine, trustrechtliche Verpflichtung zur Offenlegung der Existenz eines Trusts, wenn der Trustee für diesen tätig wird. Des Weiteren gilt zu beachten, dass im Unterschied zu anderen Rechtsformen keine zwingende Überprüfung der Identität der involvierten Personen erfolgt und sowohl der rechtliche als auch wirtschaftliche Aufwand für die Gründung und laufende Fortführung sehr gering sind. Eine lückenlose Erfassung im WiEReG kann schon aufgrund der Tatsache, dass die eigenständigen Meldungen der Trusts die einzige Erhebungsquelle darstellen, nicht sichergestellt werden.
Trustähnliche Vereinbarungen	<b>sehr hoch</b>	Für die Errichtung von trustähnlichen Vereinbarungen sind weder einheitliche Formvorschriften, noch zwingende Eintragungen in öffentliche Register vorgesehen. Auch bestehen keine prinzipiellen Mitwirkungspflichten von Notaren oder Rechtsanwälten. Des Weiteren gilt zu beachten, dass – so nicht berufsmäßige Parteienvertreter bei der Gründung beigezogen werden – keine zwingende Überprüfung der Identität der involvierten Personen erfolgt und sowohl der rechtliche als auch wirtschaftliche Aufwand für die Gründung und laufende Fortführung sehr gering sein können. Eine lückenlose Erfassung im WiEReG kann schon aufgrund der Tatsache, dass die eigenständigen Meldungen der trustähnlichen Vereinbarungen die einzige Erhebungsquelle darstellen, nicht sichergestellt werden.

**Typische in der jüngsten Vergangenheit beobachtete Bedrohungsszenarien:**

Missbrauch der Rechtsform: Ein in Zusammenhang mit **Terrorismusfinanzierung** beobachtetes Bedrohungsszenarium betrifft Vereine als mögliche Vehikel, um Gelder zum Zwecke der Terrorismusfinanzierung ins Ausland zu transferieren. Dabei handelt es sich meist um bereits seit mehreren Jahren oder Jahrzehnten bestehende Vereine, welche vermeintlich humanitäre bzw. mildtätige Ziele verfolgen, die beschafften Gelder im Ausland jedoch nicht oder nur zum Teil bei den beworbenen Hilfsprojekten ankommen. Zahlungsempfänger sind oft natürliche Personen oder ausländische Vereine in von Terrorismus stark betroffenen Ländern, wobei die Verwendung der Gelder mangels Nachweisen bzw. Aufzeichnungen nicht überprüft werden kann.

Missbrauch des Vereins durch Dritte: Nationale wohltätige Vereine sind in Krisengebieten als Hilfsorganisationen tätig und bedienen sich örtlicher Helfer, deren Hintergrund nie umfangreich abgeklärt werden kann. (Quelle: BVT).

Im Hinblick auf die **Geldwäsche** konnte als Bedrohungsszenarium die Nutzung von Gesellschaften mit beschränkter Haftung zur Verschleierung der Herkunft finanzieller Mittel ausgemacht werden. Dabei werden mehrere Firmen (bzw. speziell für diesen Zweck angekaufte Firmenmäntel) dazu verwendet, Finanzströme entlang der konstruierten Firmenkette zu schleusen. Für die beteiligten Firmen werden Scheingeschäftsführer aus dem Ausland (zumeist aus osteuropäischen Staaten) herangezogen, die gleichzeitig auch als Gesellschafter im Firmenbuch eingetragen werden, allerdings keinen Einblick in die Geschäftstätigkeit der Firma haben. Dadurch werden auch die wahren wirtschaftlichen Eigentümer verschleiert. Die involvierten GmbHs sind in der Regel in der Baubranche bzw. vermehrt auch im Handel, insbesondere innereuropäisch tätig und durch Aufträge bzw. Scheinrechnungen miteinander verbunden. Die auf diesem Wege weitergeleiteten Gelder werden schließlich in bar behoben und ins Ausland geschafft. Kennzeichnend ist, dass bei den Barbehebungen durch den Geschäftsführer oftmals eine weitere Person anwesend ist, die den Scheingeschäftsführer beaufsichtigt. Viele der zwischengeschalteten Unternehmen verfügen zumindest kurzzeitig über Arbeitnehmer, wobei es typischerweise auch zu Sozialbetrug und anschließender Insolvenz einzelner Firmen kommt. Die faktischen Geschäftsführer sind nicht greifbar. Gesellschaften mit beschränkter Haftung sind attraktiv für dieses

Bedrohungsszenarium, weil sich die Rechtsform für schnelle Firmenübernahmen besonders gut eignet. Gemäß der vom BMF veröffentlichten Liste der rechtskräftig festgestellten Scheinunternehmen handelt es sich per 26.02.2021 zudem bei mehr als der Hälfte der angeführten Unternehmen um GmbHs. (Quellen: Abt. I/9, BMF-ZL; FIU)

**Potentielle Verschleierung des wirtschaftlichen Eigentums:**

Ob tatsächlich versucht wird, wirtschaftliche Eigentümer von Rechtsträgern zu verschleiern, kann auch anhand der festgestellten Unregelmäßigkeiten im Register der wirtschaftlichen Eigentümer abgeschätzt werden (der höchste Wert ist ausschlaggebend: Vermerke/Treuhandschaften: <0,5% niedrig; <1% mittel; <1,5% hoch; >1,5% sehr hoch; Intransparente ausländische Rechtsträger: <1% niedrig; <3% mittel; <4% hoch; >5% sehr hoch):

Rechtsform	Vermerke	gemeldete Treuhandschaften	intransparente ausl. oberste Rechtsträger	Beurteilung Bedrohung
Personengesellschaften (OG, KG)	0,03%	0,43%	1,11%	<b>mittel</b>
Aktiengesellschaften*	0,32%	1,17%	7,08%	<b>sehr hoch</b>
Gesellschaften mit beschränkter Haftung	0,08%	1,49%	2,26%	<b>hoch</b>
Erwerbs- und Wirtschaftsgenossenschaften	0,00%	0,00%	0,00%	<b>niedrig</b>
Versicherungsvereine und Sparkassen	0,00%	0,00%	0,00%	<b>niedrig</b>
Europäische Rechtsformen (EWIV, SE und SCE)*	0,00%	2,38%	8,33%	<b>sehr hoch</b>
Privatstiftungen	0,63%	1,48%	0,00%	<b>hoch</b>
Sonstige Rechtsträger	0,00%	0,00%	0,00%	<b>niedrig</b>
Vereine	0,00%	0,00%	0,00%	<b>niedrig</b>
Gemeinnützige Stiftungen und Fonds	0,19%	0,40%	0,00%	<b>niedrig</b>
Trusts**	0,00%	0,00%	0,00%	<b>sehr hoch</b>
Trustähnliche Vereinbarungen**	0,00%	0,00%	0,00%	<b>sehr hoch</b>
<b>DURCHSCHNITT</b>	<b>0,10%</b>	<b>0,61%</b>	<b>1,57%</b>	

\* Aufgrund der beobachteten potentiellen Verschleierung des wirtschaftlichen Eigentums ergibt sich für **Aktiengesellschaften und europäische Rechtsformen** eine **sehr hohe** Bedrohung, wobei hier der Anteil intransparenter ausländischer oberster Rechtsträger ausschlaggebend ist, welcher deutlich über 5% liegt.

\*\* Im Hinblick auf **Trusts (bzw. trustähnliche Vereinbarungen)** gilt zu beachten, dass eine lückenlose Erfassung der in den Anwendungsbereich des WiEReG fallenden Trusts schon aufgrund der Tatsache, dass die eigenständige Eintragung im Ergänzungsregister für sonstige Betroffene die einzige Erhebungsquelle darstellt, nicht sichergestellt werden kann. Die oben genannten Zahlen lassen nur einen Schluss im Hinblick auf die Offenlegung der wirtschaftlichen Eigentümer jener Trusts zu, die im Ergänzungsregister registriert wurden. Rückschlüsse auf die Zahl jener Trusts, deren Trustees ihrer Verpflichtung zur Eintragung des Trusts im Ergänzungsregister nicht nachgekommen sind, sind daraus nicht möglich. Aufgrund der fehlenden Überprüfbarkeit ist daher von einer **sehr hohen** potentiellen Verschleierung auszugehen.

## Verletzbarkeit

### **Geldwäscherei & Terrorismusfinanzierung:**

In den zusammengefassten Szenarien der SNRA wurde die Anfälligkeit/Verletzbarkeit von juristischen Personen oder Rechtsvereinbarungen sowohl im Hinblick auf den Missbrauch für die Zwecke der Terrorismusfinanzierung als auch der Geldwäsche als hoch eingestuft. In der Folge soll eine rechtsformspezifische Verletzbarkeit abgeleitet werden. Die entsprechenden Ergebnisse werden für Geldwäsche und Terrorismusfinanzierung getrennt berechnet aber gemeinsam dargestellt, im Falle von Unterschieden sind diese an den betreffenden Stellen separat ausgewiesen.

### **(a) Risikopotential:**

Entsprechend der allgemeinen Einschätzung ist das Risikopotential entsprechend der SNRA als **hoch** anzunehmen. Es bestehen folgende rechtsformspezifischen Besonderheiten:

**Sparkassen & Versicherungsvereine:** Abweichend von der allgemeinen Einschätzung ist das Risikopotential als **niedrig** einzustufen. Aufgrund der laufenden Aufsicht durch die FMA in Kombination mit den strengen rechtlichen Anforderungen an die Gründung, die Bestellung der vertretungsbefugten Personen und die laufende Fortführung dürfte es für potentielle Täter sehr schwierig sein, diese Rechtsform für Zwecke der Terrorismusfinanzierung zu missbrauchen.

**Sonstige Rechtsträger:** Abweichend von der allgemeinen Einschätzung ist das Risikopotential als **niedrig** anzunehmen, dies aufgrund der Besonderheiten der Rechtsform im Hinblick auf deren Gründung und deren Zuordnung zum öffentlichen Sektor und der damit verbundenen Einschränkungen und Kontrollmechanismen.

**Vereine:** Abweichend von der allgemeinen Einschätzung der SNRA ist das Risikopotential als **mittel** anzunehmen, da Vereine nur für ideelle Zwecke gegründet werden dürfen und nicht auf Gewinn gerichtet sein dürfen. Aufgrund der typischen Einsatzbereiche dieser Rechtsform wird es auch nicht

möglich sein, größere Transaktionen über die Konten eines Vereins abzuwickeln, ohne dass diese im Transaktionsmonitoring der Kreditinstitute auffallen würden. Allerdings können Vereine in begrenzten Umfang zur Sammlung von Spenden eingesetzt werden. Sofern diese jedoch in zwei aufeinander folgenden Jahren eine Million Euro übersteigen, ist zwingend ein erweiterter Jahresabschluss aufzustellen sowie ein Abschlussprüfer zu bestellen. Anzumerken ist aber, dass die Möglichkeiten zur Überprüfung der tatsächlichen Verwendung der Mittel in der Praxis oft eingeschränkt sind (z.B., weil Gelder ins Ausland fließen und eine Überprüfung vor Ort nicht vorgenommen werden kann).

**Gemeinnützige Stiftungen und Fonds:** Abweichend von der allgemeinen Einschätzung der SNRA ist das Risikopotential als **mittel** anzunehmen, da gemeinnützige Stiftungen und Fonds nur für die Erfüllung gemeinnütziger oder mildtätiger Zwecke gegründet werden dürfen und nicht auf Gewinn gerichtet sein dürfen. Da Gelder nur zweckentsprechend entnommen werden dürfen und gemäß § 2 Abs. 1 BStFG sichergestellt werden muss, dass das verbleibende Vermögen Euro 50.000 nicht unterschreitet, eignet sich diese Rechtsform nicht für die Sammlung und Weiterleitung von Spenden.

**(b) Risikobewusstsein:**

Entsprechend der allgemeinen Einschätzung ist von einem **mittleren** Risikobewusstsein auszugehen. Es bestehen jedoch folgende rechtsformspezifischen Besonderheiten:

**Europäische Rechtsformen:** Da es sich um sehr selten verwendete Rechtsformen handelt, ist abweichend von der allgemeinen Einschätzung von einem **niedrigen** Risikobewusstsein auszugehen.

**Trusts und trustähnliche Vereinbarungen:** Abweichend von der allgemeinen Einschätzung ist bei diesen Rechtsträgern von einem **niedrigen** Risikobewusstsein auszugehen, da die Verwendung dieser Rechtsinstrumente in Österreich nicht üblich ist und daher das diesbezügliche Wissen der Verpflichteten nicht ausreichend sein könnte.

**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Im Hinblick auf die rechtlichen Rahmenbedingungen und die Aufsicht/Governance erfolgt eine Bewertung der rechtlichen Anforderungen an Notare und Rechtsanwälte bei der Gründung, der Governanceanforderungen und der Melde-Compliance für jede Rechtsform (die Melde-Compliance setzt sich zu gleichen Teilen aus der Meldequote und der Vermerkquote zusammen; Meldequote: >95% sehr hohe; >90% hohe; >80% mittlere; <80% niedrige Compliance; Vermerkquote: <0,05% sehr hohe; <0,1% hohe; <0,5% mittlere; >0,5% niedrige Compliance):

Rechtsform	Rechtliche Anforderungen*	Governanceanforderungen*	Meldequote	Vermerkquote	Melde-Compliance
Personengesellschaften (OG, KG)	sehr hoch	mittel	98,81%	0,03%	sehr hoch
Aktiengesellschaften	sehr hoch	sehr hoch	95,79%	0,32%	hoch

Gesellschaften mit beschränkter Haftung	sehr hoch	hoch	98,80%	0,08%	sehr hoch
Erwerbs- und Wirtschaftsgenossenschaften	sehr hoch	hoch	97,70%	0,00%	sehr hoch
Versicherungsvereine und Sparkassen	sehr hoch	sehr hoch	95,68%	0,00%	sehr hoch
Europäische Rechtsformen (EWIV, SE und SCE)	sehr hoch	hoch	74,50%	0,00%	hoch
Privatstiftungen	sehr hoch	sehr hoch	97,88%	0,63%	hoch
Sonstige Rechtsträger	sehr hoch	sehr hoch	84,84%	0,00%	hoch
Vereine**	niedrig	mittel	73,04%	0,00%	hoch
Gemeinnützige Stiftungen und Fonds	niedrig	hoch	81,08%	0,19%	mittel
Trusts	niedrig	niedrig	100,00%	0,00%	sehr hoch
Trustähnliche Vereinbarungen	niedrig	niedrig	0,00%	0,00%	niedrig
<b>DURCHSCHNITT</b>			<b>89,83%</b>	<b>0,05%</b>	

\* Nähere Informationen über die rechtlichen Anforderungen bzw. die Governanceanforderungen finden sich auch in den Ausführungen zur rechtsformspezifischen Eignung.

\*\* **Vereine** weisen mit 73,04% eine verhältnismäßig niedrige Meldequote auf, was vermutlich darauf zurückzuführen ist, dass im Jahr 2020 aufgrund von COVID-19 zahlreiche geplanten Mitgliederversammlungen nicht abgehalten werden konnten und es deshalb nicht zur Neuwahl bzw. Verlängerung der Funktionsperiode der vertretungsbefugten Organe kam, welche im Regelfall der Meldebefreiung automatisationsunterstützt in das Register der wirtschaftlichen Eigentümer übernommen werden.

#### Risikomindernde Maßnahmen

- Verpflichtung der Rechtsträger zur jährlichen Feststellung und Überprüfung der wirtschaftlichen Eigentümer sowie Meldung an das Register der wirtschaftlichen Eigentümer
- Gewährleistung der Meldepflicht durch ein automatisiertes Zwangsstrafenverfahren

- Risikoorientierte Analyse und Prüfung der eingehenden Meldungen durch die Registerbehörde und Sanktionierung von unrichtigen Meldungen mit Finanzstrafen von bis zu 200.000 Euro
- Verpflichtende Einsicht für verpflichtete Unternehmen bei Begründung einer Geschäftsbeziehung verbunden mit der Verpflichtung zur Setzung von Vermerken bei unrichtigen Meldungen
- Vielfältige Möglichkeiten zur Integration des Registers in die laufenden Prozesse bei verpflichteten Unternehmen durch eine Webservice-Anbindung und einen Änderungsdienst

### Gesamtrisiko

Die Berechnungsmethode des Gesamtrisikos stellt sich wie folgt dar: **Gesamtrisiko** = 40% Bedrohung + 60% Verletzbarkeit – risikomindernde Maßnahmen.

Das Gesamtrisiko wird aufgeschlüsselt nach den Rechtsformen in **folgender Tabelle** dargestellt (niedriges Risiko: 1-1,5; mittleres Risiko: 1,51-2,5; hohes Risiko: 2,51-3,5; sehr hohes Risiko: 3,51-4. Alle Werte mit hohem oder sehr hohem Risiko sind rot hinterlegt):

	Bedrohung*		Verletzbarkeit**		Restrisiko		Rechtsform-spezifisches Risiko	Risikomindernde Maßnahmen***	Gesamtrisiko	Einstufung
	TF	GW	TF	GW	TF	GW	TF/GW			
Personengesellschaften (OG und KG)	2,3	2,5	2,2	2,1	2,2	2,3	2,22	-0,55	1,66	mittel
Aktiengesellschaft	2,2	2,5	1,9	1,9	2,0	2,2	2,08	-0,52	1,56	mittel
Gesellschaft mit beschränkter Haftung	2,1	2,8	2,0	2,0	2,0	2,3	2,17	-0,54	1,63	mittel
Erwerbs- und Wirtschaftsgenossenschaften	1,8	2,2	1,9	1,9	1,9	2,0	1,95	-0,49	1,46	niedrig
Versicherungsvereine und Sparkassen	1,8	2,2	1,3	1,3	1,5	1,6	1,55	-0,39	1,16	niedrig
Europäische Rechtsformen (EWIV, SE und SCE)	2,2	2,5	2,4	2,4	2,3	2,5	2,38	-0,60	1,79	mittel
Privatstiftungen	2,3	2,6	2,0	2,0	2,1	2,2	2,17	-0,54	1,63	mittel
sonstige Rechtsträger	1,6	1,9	1,4	1,4	1,5	1,6	1,55	-0,39	1,16	niedrig
Vereine	1,9	1,9	2,6	2,6	2,3	2,3	2,32	-0,58	1,74	mittel
Gemeinnützige Stiftungen und Fonds	1,3	1,7	2,5	2,5	2,0	2,2	2,10	-0,53	1,58	mittel
Trusts	2,8	3,2	3,3	3,3	3,1	3,2	3,15	-0,79	2,36	mittel
trustähnliche Vereinbarungen	3,2	3,5	3,8	3,8	3,5	3,7	3,58	-	3,58	sehr hoch



\* Die **Bedrohung** wird wie folgt berechnet: Ergebnis der SNRA: 1/3, Ergebnis nationale Risikoanalyse: 2/3 (davon geografische Bedrohung, wirtschaftliche Bedrohung, rechtsformspezifische Eignung und beobachtete Bedrohungsszenarien je 1/4)

\*\* Die **Anfälligkeit/Verletzbarkeit** wird wie folgt berechnet: Risikopotential: 1/4, Risikobewusstsein: 1/4, Rechtliche Rahmenbedingungen und Aufsicht: 1/2 (davon rechtliche Anforderungen an Notare und Rechtsanwälte bei der Gründung, Governanceanforderungen und Melde-Compliance je 1/3)

\*\*\* Die Wirksamkeit der **risikomindernden Maßnahmen** wird pauschal mit 1/4 des Gesamtrisikos vor Abzug der risikomindernden Maßnahmen angenommen. Davon ausgenommen sind trustähnliche Vereinbarungen, da diese zum Stichtag 1. Jänner 2021 eine Meldequote von 0% aufgewiesen haben.

### Empfehlungen

Die Registerbehörde sollte die folgenden Maßnahmen setzen:

- Eine weitere Verbesserung der Datenqualität sollte einerseits durch eine Weiterentwicklung der risikoorientierten Aufsicht auf Basis der Ergebnisse der nationalen Risikoanalyse (interne Maßnahmen) und andererseits durch eine Verbesserung der Reaktion der verpflichteten Unternehmen auf festgestellte Unrichtigkeiten im Register der wirtschaftlichen Eigentümer (externe Maßnahmen) erreicht werden
- die rechtsformspezifischen Meldequoten sollten einem laufenden Monitoring unterzogen werden und es sollten rechtsformspezifische Maßnahmen getroffen werden
- die Integration des Registers der wirtschaftlichen Eigentümer in individuelle und standardisierte Softwareprodukte sollte weiter forciert werden, um digitale Prozesse zu ermöglichen und die praktische Handhabung des Registers zu vereinfachen
- im Hinblick auf die beobachteten Bedrohungsszenarien sollten in Zusammenarbeit mit den betroffenen Behörden risikomindernde Maßnahmen erarbeitet werden
- die Zusammenarbeit mit den Abgabenbehörden und Finanzstrafbehörden sollte intensiviert werden, um die Melde-Compliance weiter zu erhöhen
- die Zusammenarbeit mit Aufsichtsbehörden von Verpflichteten, der Geldwäschemeldestelle und des BVT sollte intensiviert werden und es sollte ein Wissenstransfer im Rahmen von Workshops stattfinden

Die Aufsichtsbehörden sollten bei der Überprüfung der Einhaltung der Sorgfaltspflichten bei verpflichteten Unternehmen ein besonderes Augenmerk auf folgende Punkte legen:

- Umsetzung der Verpflichtung zur Einsicht in das Register der wirtschaftlichen Eigentümer bei Begründung einer neuen Geschäftsbeziehung und der Aktualisierung der Daten über die wirtschaftlichen Eigentümer
- Umsetzung der Verpflichtung zur Vermerksetzung

# Sektorrisikoanalyse Finanzsektor

<b>Finanzsektor/Guthaben bei Kredit- und Finanzinstituten (KI/FI)</b>
<b>Allgemeine Informationen</b>
KI/FI bilden in vielen Fällen den ersten Anknüpfungspunkt, um Gelder in das allgemeine Finanzsystem zu bringen. Zusätzlich machen die weite Verbreitung und Zugänglichkeit sowie die relativ geringen Kosten die Dienstleistungen von KI/FI für die Nutzung von GW/TF attraktiv. Der österreichische Finanzsektor ist traditionell von einer hohen Anzahl an KI geprägt. Abgesehen von der starken Bankdurchdringung des heimischen Finanzplatzes sind österreichische KI auch in ausländischen Märkten (insbes. CESEE) sehr stark vertreten, was sich insbesondere durch die Anzahl der (ausländischen) Töchter und Zweigniederlassungen zeigt.
<b>Bedrohung</b>
<b>Terrorismusfinanzierung:</b> In den zusammengefassten Szenarien der SNRA wurde die Bedrohung, dass Guthaben bei KI/FI für terroristische Aktivitäten missbraucht werden, mit einem hohen bis sehr hohen Risiko eingestuft.  Bedrohungen bestehen, da Terroristen und deren Unterstützer das klassische Finanzsystem einerseits nutzen, um Gelder für die Unterstützung von terroristischen Aktivitäten zu sammeln – sowohl durch legale als auch durch illegale Tätigkeiten. Andererseits aber auch, um (Klein-) Beträge in Gebiete zu überweisen, in denen terroristische Handlungen ausgeführt werden sollen.  <b>Conclusio:</b> <b>Zusammenfassend ist die Bedrohung mit hoch einzustufen.</b>
<b>Geldwäscherei:</b> In den zusammengefassten Szenarien der SNRA wurde die Bedrohung mit einem sehr hohen Risiko eingestuft.  Aufgrund der Vielzahl der von KI/FI angebotenen Finanzprodukte und -dienstleistungen sowie der Abwicklung des Zahlungsverkehrs besteht in diesem Zusammenhang ein besonderes Risiko, für Zwecke der Geldwäscherei missbraucht zu werden. Vor allem Transaktionen im Zusammenhang mit Bargeld, Prepaidkarten und geldnahen Finanzanlagen (z.B. Termingelder, Einlagen) mit hoher Liquidität führen zu einem erhöhten Risiko. Andere Kontoarten, wie z.B. bestimmte Formen von Anderkonten (vgl. AndKo-SoV) oder Schulsparkonten (vgl. Schulspar-SoV) können mit einem geringeren Risiko verbunden sein.  <b>Conclusio:</b> <b>Zusammenfassend ist die Bedrohung mit hoch einzustufen.</b>
<b>Verletzbarkeit</b>
<b>Terrorismusfinanzierung:</b> In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von Guthaben bei KI/FI im Hinblick auf den Missbrauch für die Zwecke der Terrorismusfinanzierung mit hoch eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden.

**(a) Risikopotential:**

Von der FMA werden Daten zu allen Transaktionen in und aus allen Ländern der Welt erhoben (diese Daten beziehen sich dabei auf jedes einzelne Land und erfassen sowohl alle Ein- als auch Ausgänge). Bezogen auf das gesamte Transaktionsvolumen des österreichischen Finanzmarktes wird nur ein geringer Teil in Hochrisikoländer oder Krisengebiete (bzw. angrenzende Länder) durchgeführt oder stammt aus solchen Ländern.

**(b) Risikobewusstsein:**

Die Daten der FMA zeigen auch, dass nur eine kleine Anzahl an KI/FI derartige Transaktionen durchführt.

**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Geschäftsbeziehungen und Transaktionen, an denen Hochrisikoländer beteiligt sind, führen gemäß § 9a FM-GwG dazu, dass solche Kunden im hohen Risiko zu führen und zusätzlich zu den jedenfalls anzuwendenden Sorgfaltspflichten weitere verstärkte Sorgfaltspflichten anzuwenden sind. Darüber hinaus sind bei der Risikoeinstufung eines Kunden jedenfalls auch die in Anlage III zu § 9 FM-GwG aufgezählten risikoe erhöhende Faktoren zu berücksichtigen.

**Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine hohe Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von Guthaben bei KI/FI, für die Zwecke der Terrorismusfinanzierung missbraucht zu werden, mit mittel einzustufen ist.**

**Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von Guthaben bei KI/FI im Hinblick auf den Missbrauch für die Zwecke der Geldwäscherei mit hoch eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden.

**(a) Risikopotential:**

Die österreichische Struktur an KI/FI ist sehr heterogen und bedient eine Vielzahl unterschiedlicher Kunden- und Geschäftssegmente. Diese reichen vom regional beschränkten, klassischen Retail- und Kommerzgeschäft, über das internationale Corporate- und Investmentbanking, bis hin zum internationalen Private Banking.

**(b) Risikobewusstsein:**

Der österreichische Finanzmarkt deckt ein breitgefächertes Kundenspektrum ab. Darunter befinden sich u.a. auch Geschäftsbeziehungen zu Off-Shore-Kunden, ausländische Korrespondenzbankbeziehungen, Geschäftsbeziehungen zu politisch exponierten Personen (PEPs), Stiftungen, NPOs oder sonstige Kundenbeziehungen, die ausgehend von ihrer Typologie ein erhöhtes Risiko aufweisen können (wie etwa Geschäftsbeziehungen zu Kunden aus Regionen mit einem erhöhten geographischen Risiko). Als internationaler Bankenplatz ist Österreich traditionell auch für ausländische Kunden attraktiv.

**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Siehe dazu bereits oben zu TF.

<b>Conclusio:</b> Ausgehend von den zusammengefassten Szenarien der SNRA, die eine hohe Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von Guthaben bei KI/FI, für die Zwecke der Geldwäscherei missbraucht zu werden, mit hoch einzustufen ist.
<b>Risikomindernde Maßnahmen</b>
Aufgrund der Größe des KI/FI-Sektors in Österreich und dessen Bedeutung für den österreichischen Finanzmarkt sowie des beschriebenen GW/TF-Risikos steht dieser Sektor im Fokus der Aufsicht durch die FMA. Dies spiegelt sich insbesondere auch in der Anzahl der Aufsichtsmaßnahmen in diesem Bereich wider. Die Art und Intensität dieser Maßnahmen orientiert sich dabei u.a. an den spezifischen Risikoprofilen der KI/FI. Somit wird beim Einsatz von aufsichtsrechtlichen Maßnahmen eine risikobasierte Differenzierung zwischen allen KI/FI sichergestellt. Neue Entwicklungen und Methoden, die im Bereich GW/TF auftauchen, werden durch A-FIU und FMA mit den KI/FI im Rahmen von gemeinsamen Veranstaltungen präsentiert und diskutiert. Zusätzlich erfolgt ein vertiefter Informationsaustausch im Wege eines neuen Public-Private-Partnership Projektes.
<b>Gesamtrisiko</b>
Zusammenfassend ist das Gesamtrisiko sowohl für TF als auch für GW als hoch einzustufen.
<b>Empfehlungen</b>
Weitere verstärkte Zusammenarbeit zwischen den Behörden und den Stakeholdern, um sowohl auf aktuelle Muster und Trends hinzuweisen als auch die Erfahrungen im Rahmen der Weiterentwicklung der entsprechenden rechtlichen Grundlagen zu berücksichtigen.

<b>Finanzsektor/Kapitalanlagegesellschaften (KAG) – Immobilien- Kapitalanlagegesellschaften (Immo-KAG) – Alternative Investmentfonds Manager (AIFM)</b>
<b>Allgemeine Informationen</b>
Kapitalanlagegesellschaften (KAG) nach dem InvFG 2011 und Immo-KAG nach dem ImmoInvFG, fallen in Österreich zwar formal unter den Begriff der KI, da die Verwaltung von Investmentfonds und Immobilienfonds gemäß InvFG/ImmoInvFG als Bankgeschäft nach dem Bankwesengesetz (BWG) normiert wird. Jedoch kommt den KAG und Immo-KAG insofern eine gewisse Sonderstellung zu, als diese ausschließlich zur Erbringung von Dienstleistungen iZm der Verwaltung von Investmentfonds bzw. zur individuellen Portfolioverwaltung nach dem WAG 2018 berechtigt sind. Zusätzlich sieht das AIFMG eine Konzessionierung bzw. Registrierung für Verwalter von AIF vor. Sowohl KAG/Immo-KAG als auch – konzessionierte und registrierte – AIFM sind Verpflichtete des FM-GwG und haben die Sorgfalts- und Meldepflichten zur Prävention von GW/TF vollumfänglich einzuhalten. Kunden von KAG/Immo-KAG benötigen eine depotführende Stelle, bei der es sich um ein konzessioniertes KI handeln muss. Insbes. die Herkunft der zu investierenden Mittel werden daher in einem ersten Schritt bereits durch das depotführende KI überprüft bzw. erfüllt.
<b>Bedrohung</b>
<b>Terrorismusfinanzierung:</b> In den zusammengefassten Szenarien der SNRA wurde die Bedrohung, dass KAG, Immo-KAG und AIFM für terroristische Aktivitäten missbraucht werden, mit einem niedrigen Risiko eingestuft.

Aus der derzeitigen Informations- und Datenlage ergeben sich auch in Österreich keine konkreten Hinweise auf eine diesbezügliche Bedrohungslage.

**Conclusio:**

**Zusammenfassend ist die Bedrohung mit niedrig einzustufen.**

**Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Bedrohung mit einem hohen Risiko eingestuft.

Bei Investitionen in Investmentfonds, Immobilienfonds und Alternative Investmentfonds kann sich eine Gefahr des Missbrauches für Zwecke der Geldwäscherei vor allem im Zusammenhang mit gut ausgebildeten Personen(-gruppen) ergeben, die solche Investitionen und die dabei notwendigen Transaktionen bewusst für die Verschleierung der ursprünglichen Mittelherkunft missbrauchen.

**Conclusio:**

**Zusammenfassend ist die Bedrohung mit mittel einzustufen.**

**Verletzbarkeit**

**Terrorismusfinanzierung:**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von KAG, Immo-KAG und AIFM im Hinblick auf den Missbrauch für die Zwecke der Terrorismusfinanzierung mit niedrig eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden.

Aus der Aufsichtspraxis der FMA und den vorliegenden Daten und Informationen ergibt sich, dass Dienstleistungen und Produkte im Bereich von KAG/Immo-KAG und AIFM derzeit zu keiner besonderen Verletzbarkeit des österreichischen Finanzmarktes, für Zwecke der Terrorismusfinanzierung missbraucht zu werden, führen.

**Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine niedrige Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von KAG, Immo-KAG und AIFM, für die Zwecke der Terrorismusfinanzierung missbraucht zu werden, mit niedrig einzustufen ist.**

**Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von KAG, Immo-KAG und AIFM im Hinblick auf den Missbrauch für die Zwecke der Geldwäscherei mit mittel bis hoch eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden.

**(a) Risikopotential:**

Die Aufsichtspraxis der FMA und die erhobenen Daten und Informationen zeigen, dass Dienstleistungen und Produkte im Bereich von KAG/Immo-KAG und AIFM zu keiner über die oben beschriebene Bedrohungslage hinausgehende besondere Verletzbarkeit des österreichischen Finanzmarktes, für Zwecke der Geldwäscherei missbraucht zu werden, führen.

**(b) Risikobewusstsein:**

Wie sich aus den Daten der FMA ergibt, ist der Markt in Österreich im Bereich KAG/Immo-KAG und AIFM verhältnismäßig klein.

**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

KAG/Immo-KAG und – konzessionierte und registrierte – AIFM sind Verpflichtete des FM-GwG und unterliegen der diesbezüglichen Aufsicht der FMA. Bei der Erbringung von Dienstleistungen durch KAG/Immo-KAG und AIFM spielt das KYC-Profil eines Kunden eine wesentliche Rolle. Zwar können ungewöhnliche Transaktionen oder Aktivitäten auch in diesem Bereich gewissen Typologien folgen, jedoch ist es gerade bei Dienstleistungen von KAG/Immo-KAG und AIFM wichtig, dass die verpflichteten Institute über ausreichend Kenntnisse über ihre Kunden und deren Veranlagungsprofil verfügen. Neben dem Investitionsverhalten des Kunden ist auch auf die anschließende Verfügung (z.B. Auszahlung) über die veranlagten Vermögenswerte Bedacht zu nehmen.

**Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine mittlere bis hohe Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von KAG, Immo-KAG und AIFM, für die Zwecke der Geldwäscherei missbraucht zu werden, mit mittel einzustufen ist.**

**Risikomindernde Maßnahmen**

KAG/Immo-KAG und AIFM sind als Verpflichtete des FM-GwG von den Aufsichtsmaßnahmen der FMA erfasst. Dabei führt die FMA Vor-Ort-Maßnahmen zur Prävention von GW/TF einerseits direkt bei den genannten Verpflichteten durch, andererseits auch bei den depotführenden Banken und den Depotbanken. In diesem Zusammenhang setzt die FMA bei den depotführenden Banken und bei den Depotbanken gezielt Schwerpunkte auf den Bereich Investitionen in Investmentfonds, Immobilienfonds und Alternative Investmentfonds.

**Gesamtrisiko**

**Zusammenfassend ist das Risiko für TF als niedrig und für GW als mittel einzustufen.**

**Empfehlungen**

Weitere verstärkte Zusammenarbeit zwischen den Behörden und den Stakeholdern, um sowohl auf aktuelle Muster und Trends hinzuweisen als auch die Erfahrungen im Rahmen der Weiterentwicklung der entsprechenden rechtlichen Grundlagen zu berücksichtigen.

**Finanzsektor/Wertpapierfirmen (WPF) und Wertpapierdienstleistungsunternehmen (WPDFU)**

**Allgemeine Informationen**

Neben den KI sind bei der Erbringung von Wertpapierdienstleistungen WPF/WPDFU, die zur gewerblichen Erbringung von Wertpapierdienstleistungen nach dem WAG 2018 berechtigt sind, von Relevanz. Viele Wertpapierdienstleister bedienen sich bei der Erbringung von Wertpapierdienstleistungen und im Vertrieb externer Vermittler, die als Erfüllungsgehilfen (vertraglich gebundene Vermittler bzw. Wertpapiervermittler) für den Wertpapierdienstleister tätig werden.

## Bedrohung

### **Terrorismusfinanzierung:**

In den zusammengefassten Szenarien der SNRA wurde die Bedrohung, dass WPDLU bzw. WPF für terroristische Aktivitäten missbraucht werden, mit einem niedrigen Risiko eingestuft.

Aus der derzeitigen Informations- und Datenlage ergeben sich auch in Österreich keine konkreten Hinweise auf eine diesbezügliche Bedrohungslage.

### **Conclusio:**

**Zusammenfassend ist die Bedrohung mit niedrig einzustufen.**

### **Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Bedrohung mit einem hohen Risiko eingestuft.

Bereits bei der Wertpapierdienstleistung gem. dem WAG 2018 sind eine Vielzahl von Wohlverhaltensregeln – unabhängig der Bestimmungen im FM-GwG – im Vorfeld einzuhalten, wodurch ein umfassendes Kundenprofil bereits erstellt wird. Da aber auch Kunden wie z.B. Privatstiftungen, Kunden aus Drittstaaten etc., betreut werden, ist hier ein entsprechendes Restrisiko vorhanden.

### **Conclusio:**

**Zusammenfassend ist die Bedrohung mit mittel einzustufen.**

## Verletzbarkeit

### **Terrorismusfinanzierung:**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von WPDLU bzw. WPF im Hinblick auf den Missbrauch für die Zwecke der Terrorismusfinanzierung mit niedrig eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden.

Aus der Aufsichtspraxis der FMA und den vorliegenden Daten und Informationen ergibt sich, dass Dienstleistungen und Produkte im Bereich der Wertpapierdienstleistung derzeit zu keiner besonderen Verletzbarkeit des österreichischen Finanzmarktes, für Zwecke der Terrorismusfinanzierung missbraucht zu werden, führen.

### **Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine niedrige Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von WPDLU bzw. WPF, für die Zwecke der Terrorismusfinanzierung missbraucht zu werden, mit niedrig einzustufen ist.**

### **Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von WPDLU/WPF im Hinblick auf den Missbrauch für die Zwecke der Geldwäscherei mit hoch eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden.

### **(a) Risikopotential:**

Bei der Erbringung von Wertpapierdienstleistungen spielt sowohl das Anlegerprofil sowie das KYC-Profil eines Kunden eine wesentliche Rolle. Ungewöhnliche Transaktionen oder Aktivitäten können im gegenständlichen Bereich gewissen Typologien folgen.

**(b) Risikobewusstsein:**

Aufgrund der unterschiedlichen (persönlichen) Gegebenheiten eines jeden Anlegers ist es wichtig, dass Wertpapierdienstleister über ausreichend Kenntnisse über ihre Kunden, deren finanzielle Verhältnisse und deren Veranlagungsprofil verfügen, um so allfällige Abweichungen vom zu erwartenden Verhalten bzw. Transaktionen ohne erkennbaren wirtschaftlichen Nutzen bestmöglich erkennen zu können. Neben dem Investitionsverhalten des Kunden wird der Fokus jedenfalls auf die anschließende Verfügung (z.B. Auszahlung) über die veranlagten Vermögenswerte zu richten sein. In diesem Zusammenhang unterliegen vor allem Investments mit kurzem Veranlagungshorizont sowie fehlende Sensibilität bei anfallenden Kosten einem erhöhten Risiko.

**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Durch die Vorgaben des WAG 2018 wird eine Fülle von Informationen über den Kunden eingeholt. Unabhängig davon sind durch WPDLU/WPF auch die Bestimmungen des FM-GwG einzuhalten und eine entsprechende risikobasierte Überprüfung durchzuführen. Erst wenn diese umfassende Analyse durchgeführt wurde, kommt es zum eigentlichen Geschäft, wobei auch hier wieder die depot- und/oder kontoführende Bank des Investors abschließend eine Prüfung durchzuführen hat. WPDLU/WPF ist das Halten von Kundengeldern *ex lege* untersagt. Somit wird jede Kontoeröffnung oder Transaktion von der depot- und/oder kontoführenden Bank des Investors gegengeprüft.

**Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine hohe Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von WPDLU bzw. WPF, für die Zwecke der Geldwäscherei missbraucht zu werden, mit mittel einzustufen ist.**

**Risikomindernde Maßnahmen**

Aufgrund der Größe des Wertpapierdienstleistungssektors in Österreich und dessen Bedeutung für den österreichischen Finanzmarkt sowie des beschriebenen GW/TF-Risikos steht dieser Sektor im Fokus der Aufsicht durch die FMA. Dies spiegelt sich insbesondere auch durch entsprechende Vor-Ort-Prüfungen in diesem Bereich wider. Gewerbliche Vermögensberater (§ 136a GewO) und Wertpapiervermittler (§ 136b GewO) unterliegen einer laufenden gesetzlichen Weiterbildungsverpflichtung, die zwingend auch das Thema Geldwäscheprävention umfasst.

**Gesamtrisiko**

**Zusammenfassend ist das Risiko für TF als niedrig und für GW als mittel einzustufen.**

**Empfehlungen**

Weitere verstärkte Zusammenarbeit zwischen den Behörden und den Stakeholdern, um sowohl auf aktuelle Muster und Trends hinzuweisen als auch die Erfahrungen im Rahmen der Weiterentwicklung der entsprechenden rechtlichen Grundlagen zu berücksichtigen.



## Finanzsektor/Private Banking-Vermögensverwaltung

### Allgemeine Informationen

Im Rahmen des sogenannten *Private Banking* werden vor allem gehobene Privatkunden, die Vermögenswerte (Schwellenwert ab EUR 700.000) veranlagen, betreut. Solche Dienstleistungen umfassen oftmals auch das Anbieten von komplexen Produkten, die Durchführung von Transaktionen mit hohem Volumen und ein großes Maß an Diskretion/Vertraulichkeit hinsichtlich der Geschäftsbeziehung.

### Bedrohung

#### **Terrorismusfinanzierung:**

Aus der derzeitigen Informations- und Datenlage ergeben sich keine konkreten Hinweise auf eine Bedrohungslage.

#### **Conclusio:**

**Zusammenfassend ist die Bedrohung mit niedrig einzustufen.**

#### **Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Bedrohung mit einem hohen bis sehr hohen Risiko eingestuft.

*Private Banking*-Kundensegmente können insbesondere von folgenden Eigenschaften gekennzeichnet sein: ein hohes Transaktions- und/oder Veranlagungsvolumen; die Verwendung von komplexen Produkten und Dienstleistungen; die Verwendung von juristischen Personen mit komplexen, undurchsichtigen Eigentums- und Kontrollstrukturen (unter Umständen mit Verbindungen zu Offshore-Gebieten – in vielen Fällen aus Gründen der Steueroptimierung) sowie die Erwartung des Kunden an erhöhte Vertraulichkeit und Diskretion. Dienstleistungen und Produkte im Bereich des *Private Bankings* sind auch vor dem Hintergrund der Risikofaktoren „Kunde“ und „geographische Gebiete“ einem erhöhten Risiko, für Geldwäscherei missbraucht zu werden, ausgesetzt. Zielgruppe sind vermögende Privatkunden mit einem – im Vergleich zum klassischen Retail-Geschäft – verhältnismäßig hohen Anteil an – auch ausländischen – politisch exponierten Personen. Durch die Verwendung von komplexen, über mehrere Kaskaden aufgeteilten Gesellschaftskonstruktionen, die oftmals Verbindungen zu Offshore-Gebieten aufweisen, wird die lückenlose Nachverfolgung der Herkunft der eingesetzten Mittel und der tatsächlichen wirtschaftlichen Eigentümer dieser juristischen Personen zusätzlich erschwert.

#### **Conclusio:**

**Zusammenfassend ist die Bedrohung mit hoch einzustufen.**

### Verletzbarkeit

#### **Terrorismusfinanzierung:**

Aus der Aufsichtspraxis der FMA und den vorliegenden Daten und Informationen ergibt sich, dass Dienstleistungen und Produkte im Bereich des *Private Bankings* derzeit zu keiner besonderen Verletzbarkeit des österreichischen Finanzmarktes, für Zwecke der Terrorismusfinanzierung missbraucht zu werden, führen.

#### **Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die keine Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von**

**Dienstleistungen und Produkten im Bereich des *Private Bankings*, für die Zwecke der Terrorismusfinanzierung missbraucht zu werden, mit niedrig einzustufen ist.**

**Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von Dienstleistungen und Produkten im Bereich des *Private Bankings* im Hinblick auf den Missbrauch für die Zwecke der Geldwäscherei mit hoch bis sehr hoch eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden.

**(a) Risikopotential:**

Bezogen auf den gesamten österreichischen Finanzmarkt stellt der *Private Banking* Bereich einen relativ geringen Anteil dar. Basierend auf den von der FMA erhobenen Daten lässt sich eine Konzentration der *Private Banking* Kunden auf wenige Verpflichtete ableiten.

**(b) Risikobewusstsein:**

Bezogen auf das Teilrisiko *Private Banking* befinden sich 19 % der Verpflichteten in der niedrigen, 69 % in der mittleren und 2 % in der hohen Risikoklasse.

**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Die private Vermögensverwaltung und das *Private Banking* stellen gemäß Anlage III zu § 9 FM-GwG risikoerhöhende Faktoren dar. Verpflichtete, die Dienstleistungen und Produkte im Bereich des *Private Banking* anbieten, müssen dies sowohl auf Ebene ihrer Unternehmens- als auch ihrer Kundenrisikoanalyse berücksichtigen und haben entsprechende risikomindernde Maßnahmen zu setzen. Dazu zählen z.B. zusätzliche Informationen und vertiefende Dokumente zum wirtschaftlichen Eigentümer des Kunden, zur Herkunft der eingesetzten Mittel und zu Zweck und Art der Geschäftsbeziehung (dies kann etwa dann besonders relevant sein, wenn es sich um Kunden aus Offshore-Gebieten handelt, die keine weiteren Anknüpfungspunkte zu Österreich aufweisen und/oder keinen operativen Tätigkeiten nachgehen). Außerdem haben Institute bei solchen Kunden eine intensivere kontinuierliche Überwachung der Geschäftsbeziehung (und der Transaktionen) sicherzustellen und die Intervalle für die Aktualisierung der eingeholten Unterlagen/Informationen zu verkürzen.

**Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine hohe bis sehr hohe Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von Dienstleistungen und Produkten im Bereich des *Private Bankings*, für die Zwecke der Geldwäscherei missbraucht zu werden, mit mittel bis hoch einzustufen ist.**

**Risikomindernde Maßnahmen**

Eine hohe Anzahl an *Private Banking*-Kunden im Verhältnis zum Gesamtkundenbestand stellt im Rahmen der Risikoklassifizierung einen risikoerhöhenden Faktor dar. Durch die Einstufung in eine höhere Risikokategorie kommt es zu einer intensiveren Überwachung durch die FMA und verkürzt sich dadurch auch das Intervall an Aufsichtsmaßnahmen durch die FMA entsprechend, bis hin zu jährlichen Aufsichtsmaßnahmen. Die FMA führte und führt spezielle Vor-Ort-Prüfungen mit Fokus auf das *Private Banking* Kundensegment bei den betroffenen Verpflichteten durch. In diesem Zusammenhang bilden insbesondere auch die Einhaltung der Sorgfaltspflichten zur Feststellung der Identität der wirtschaftlichen Eigentümer des Kunden und zur Einholung und Überprüfung von Informationen über die Herkunft der eingesetzten Mittel einen Schwerpunkt.

<b>Gesamtrisiko</b>
Zusammenfassend ist das Risiko für TF als niedrig und für GW als mittel bis hoch einzustufen.
<b>Empfehlungen</b>
Weitere verstärkte Zusammenarbeit zwischen den Behörden und den Stakeholdern, um sowohl auf aktuelle Muster und Trends hinzuweisen als auch die Erfahrungen im Rahmen der Weiterentwicklung der entsprechenden rechtlichen Grundlagen zu berücksichtigen.

<b>Finanzsektor/Crowdfunding</b>
<b>Allgemeine Informationen</b>
<p>Für die aufsichtsrechtliche Beurteilung von Crowdfunding im weiteren Sinne ist es von Bedeutung, wie die Form der Finanzierung im Detail ausgestaltet ist. Donation- oder reward-based Crowdfunding ist grundsätzlich nur dort von den österreichischen finanzmarktrechtlichen Aufsichtsgesetzen betroffen, wo die Plattform auch die Zahlungsabwicklung zwischen den Investoren und den Projekten unternimmt. In diesem Fall kann eine Konzession nach ZaDiG 2018 erforderlich sein. Hingegen hängt beim Betrieb einer Crowdinvesting-Plattform die Konzessionspflicht von der Art des Investments einerseits und der Art der Plattfortmätigkeit andererseits ab (z.B. Kreditvermittlungsplattformen oder wenn das Investment als Einlagengeschäft ausgestaltet ist [Konzession nach dem BWG]; Plattformen, die übertragbare Wertpapiere oder sonstige Finanzinstrumente vermitteln oder persönliche Anlageempfehlungen abgeben [Konzession nach dem WAG 2018]). Bei Projekten, bei denen die entgegennehmende Gesellschaft in weitere Gesellschaften investiert und selbst nicht operativ tätig ist, kann regelmäßig das Alternative Investmentfonds Manager Gesetz (AIFMG) zur Anwendung kommen. Fällt ein Crowdfunding-Projekt oder der Betrieb einer Crowdinvesting-Plattform unter eines der o.g. Aufsichtsgesetze, handelt es sich beim Anbieter/Betreiber grundsätzlich auch um einen Verpflichteten des FM-GwG. Für Crowdinvestments, die nach dem AltFG begeben werden, enthält das AltFG Pflichten für Plattformen. Fällt der Betreiber der Plattform nicht unter die Bestimmungen des FM-GwG, sind die Bestimmungen zur Prävention von GW/TF der Gewerbeordnung (GewO) gemäß den §§ 365m bis 365z anzuwenden (§ 5 Abs. 2 Z 1 AltFG). Das betrifft insbesondere das Crowdinvesting in Form von Veranlagungen, wofür zumindest eine Gewerbeberechtigung für die Gewerbliche Vermögensberatung gemäß § 136a GewO notwendig ist (§ 5 Abs. 1 AltFG). Ebenso enthält das AltFG Pflichten für jene Emittenten, die sich nicht ausschließlich einer Plattform bedienen (§ 4 Abs. 5 AltFG). Die diesbezügliche Beaufsichtigung fällt in diesem Bereich unter die Zuständigkeit der Gewerbebehörden.</p>
<b>Bedrohung</b>
<p><b>Terrorismusfinanzierung:</b></p> <p>In den zusammengefassten - alle Formen von Crowdfunding im weiteren Sinne, also auch donation- und reward-based Crowdfunding umfassenden - Szenarien der SNRA wurde die Bedrohung, dass Crowdfunding in bestimmten Formen für terroristische Aktivitäten missbraucht wird, mit einem mittleren Risiko eingestuft.</p> <p>Insbesondere der nicht regulierte „donation-based“ Crowdfunding-Bereich kann mit relativ einfachen Mitteln für Zwecke der Terrorismusfinanzierung missbraucht werden. Terroristen oder deren Unterstützer können diese Möglichkeiten des Crowdfunding nutzen, um Gelder für terroristische Zwecke oder zur Unterstützung terroristischer Aktivitäten zu sammeln. Aus</p>

der vorliegenden Informations- und Datenlage können sich derartige Bedrohungslagen auch in Österreich ergeben.

**Conclusio:**

**Zusammenfassend ist die Bedrohung für den reglementierten Bereich mit mittel und für den nicht reglementierten Bereich (donation-based, reward-based) mit mittel bis hoch einzustufen.**

**Geldwäscherei:**

In den zusammengefassten - alle Formen von Crowdfunding im weiteren Sinne, also auch donation- und reward-based Crowdfunding umfassenden - Szenarien der SNRA wurde die Bedrohung mit einem mittleren Risiko eingestuft. Aus der derzeitigen Informations- und Datenlage ergeben sich keine konkreten Hinweise auf eine Bedrohungslage in Österreich, wonach Crowdfunding für Zwecke der Geldwäscherei missbraucht wird.

**Conclusio:**

**Zusammenfassend ist die Bedrohung mit mittel einzustufen.**

**Verletzbarkeit**

**Terrorismusfinanzierung:**

In den zusammengefassten - alle Formen von Crowdfunding im weiteren Sinne, also auch donation- und reward-based Crowdfunding umfassenden - Szenarien der SNRA wurde die Verletzbarkeit von bestimmten Formen von Crowdfunding im Hinblick auf den Missbrauch für die Zwecke der Terrorismusfinanzierung mit mittel eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden.

**(a) Risikopotential:**

In Österreich besteht ein weites Netz an aufsichtsrechtlichen Bestimmungen, die im Zusammenhang mit Crowdfunding Projekten oder Plattformen zur Anwendung gelangen könnten. In diesen Fällen ist der Betreiber im Bereich der Finanzmarktaufsichtsgesetze hinsichtlich der Prävention von GW/TF von der FMA beaufsichtigt. Im Falle einer Anwendung des AltFG sind die Gewerbebehörden dafür zuständig.

**(b) Risikobewusstsein:**

In jenen Fällen, die unter keine der o.g. Aufsichtsgesetze fallen, ist für den Weitertransfer der eingesammelten Gelder in den meisten Fällen ein beaufsichtigter Finanzmarktintermediär notwendig. Als Verpflichtete der Sorgfaltspflichten zur Prävention von GW/TF haben diese insbesondere bei Einzahlung von höheren Barbeträgen oder bei Eingängen von vielen Kleinbeträgen innerhalb eines kurzen Zeitraums, die schnell zu einer hohen Gesamtsumme führen, sehr genau auf die Mittelherkunft zu achten.

**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Betreiber von Crowdfunding Projekten oder Plattformen haben, wenn sie Verpflichtete des FM-GwG sind oder, wenn das AltFG anwendbar ist, die jeweils anwendbaren Sorgfalts- und Meldepflichten vollumfänglich anzuwenden. KI/FI haben als Verpflichtete des FM-GwG insbesondere auch bei (Bar-)Einzahlungen von höheren Beträgen (dies stellt jedenfalls einen risikoe erhöhenden Faktor dar), zusätzliche Informationen und Nachweise zur Mittelherkunft einzuholen. Dies ist vor allem auch für jenen Bereich eine wichtige risikomindernde Maßnahme, in dem Crowdfunding Projekte oder Plattformen keiner Regulierung unterliegen und bei denen durch das Einsammeln von kleineren Beträgen Gelder für terroristische Zwecke eingesammelt werden sollen.

**Conclusio:**

Ausgehend von den zusammengefassten Szenarien der SNRA, die eine mittlere Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von Crowdfunding im weiteren Sinne, für die Zwecke der Terrorismusfinanzierung missbraucht zu werden, für den reglementierten Bereich mit mittel und für den nicht reglementierten Bereich mit mittel bis hoch einzustufen ist.

**Geldwäscherei:**

In den zusammengefassten - alle Formen von Crowdfunding im weiteren Sinne, also auch donation- und reward-based Crowdfunding umfassenden - Szenarien der SNRA wurde die Verletzbarkeit von Crowdfunding im Hinblick auf den Missbrauch für die Zwecke der Geldwäscherei mit mittel eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden.

Aus der Aufsichtspraxis der FMA und den vorliegenden Daten und Informationen ergibt sich keine darüberhinausgehende Verletzbarkeit des österreichischen Finanzmarktes.

**Conclusio:**

Ausgehend von den zusammengefassten Szenarien der SNRA, die eine mittlere Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von Crowdfunding im weiteren Sinne, für die Zwecke der Geldwäscherei missbraucht zu werden, mit mittel einzustufen ist.

**Risikomindernde Maßnahmen**

Die von den finanzmarktrechtlichen Aufsichtsgesetzen erfassten Betreiber von Crowdfunding Projekten oder Plattformen werden als Verpflichtete des FM-GwG von der FMA hinsichtlich der Einhaltung der Sorgfaltspflichten zur Prävention von GW/TF beaufsichtigt. Darüber hinaus überwachen die zuständigen Gewerbebehörden die Einhaltung der diesbezüglichen Verpflichtungen aus dem AltFG bzw. der GewO in jenen Fällen, in denen das AltFG zur Anwendung gelangt.

**Gesamtrisiko**

**Zusammenfassend ist das Risiko für TF für den reglementierten Bereich als mittel, für den nicht reglementierten Bereich als mittel bis hoch und für GW als mittel einzustufen.**

**Empfehlungen**

Weitere verstärkte Zusammenarbeit zwischen den Behörden und den Stakeholdern, um sowohl auf aktuelle Muster und Trends hinzuweisen als auch die Erfahrungen im Rahmen der Weiterentwicklung der entsprechenden rechtlichen Grundlagen zu berücksichtigen.

**Finanzsektor/Wechselstuben**

**Allgemeine Informationen**

Wechselstuben können insbesondere dazu verwendet werden, um (inkriminierte) Gelder in höher denominierte Geldscheine zu wechseln. Dieser Vorgang kann einen ersten Schritt im Zusammenhang mit grenzüberschreitenden Bargeldtransporten darstellen. Für die Durchführung eines Geldwechsels bedarf es keiner größeren Vorbereitungen oder Planungen und kann ein solcher daher relativ einfach durchgeführt werden.

## Bedrohung

### **Terrorismusfinanzierung:**

In den zusammengefassten Szenarien der SNRA wurde die Bedrohung, dass Wechselstuben für terroristische Aktivitäten missbraucht werden, mit einem hohen Risiko eingestuft.

Vor allem in grenznahen Gebieten und an Flughäfen können Terroristen und deren Unterstützer Wechselstuben nutzen, um Bargeld nach einem Wechsel in höher denominierte Geldscheine für die Unterstützung von terroristischen Gruppen und Aktivitäten in Krisengebiete zu transportieren. Ein erhöhtes Risiko ergibt sich in diesem Zusammenhang allerdings nur, wenn sich Wechselstuben in einem grenznahen Bereich zu Krisengebieten befinden.

### **Conclusio:**

**Zusammenfassend ist die Bedrohung mit mittel bis hoch einzustufen.**

### **Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Bedrohung mit einem hohen Risiko eingestuft.

Wechselstuben können dazu missbraucht werden, inkriminierte (ausländische) Gelder in – unter Umständen höher denominierte – Euro-Beträge zu wechseln.

### **Conclusio:**

**Zusammenfassend ist die Bedrohung mit mittel bis hoch einzustufen.**

## Verletzbarkeit

### **Terrorismusfinanzierung:**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von Wechselstuben im Hinblick auf den Missbrauch für die Zwecke der Terrorismusfinanzierung mit hoch eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden.

#### **(a) Risikopotential:**

Aufgrund der geographischen Lage Österreichs besteht nur ein geringer Anreiz, ausländische Gelder (Valuten) über Wechselstuben in Österreich in höher denominierte Euro-Geldbeträge zu wechseln. Die allfälligen Transportwege für eine Nutzung zu terroristischen Zwecken in Krisengebiete wären lang und bietet dies daher wenig Anreiz für Terroristen oder deren Unterstützer. Jedoch können ausländische Gelder (Valuten) über Wechselstuben in Euro-Beträge gewechselt werden, die in weiterer Folge für die Finanzierung von terroristischen Aktivitäten in Österreich verwendet werden.

#### **(b) Risikobewusstsein:**

Durch die Abschaffung der Neuausgabe der 500-Euro-Banknote mit 26.04.2019 wird der Anreiz, größere Geldbeträge in Euro-Bargeld zu transportieren, sukzessive verringert.

#### **(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Als Verpflichtete des FM-GwG haben Wechselstuben die diesbezüglichen Sorgfalts- und Meldepflichten vollumfänglich anzuwenden.

### **Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine hohe Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit**

**von Wechselstuben, für die Zwecke der Terrorismusfinanzierung missbraucht zu werden, mit mittel bis hoch einzustufen ist.**

**Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von Wechselstuben im Hinblick auf den Missbrauch für die Zwecke der Geldwäscherei mit hoch eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden.

**(a) Risikopotential:**

Um inkriminierte Gelder, die über eine Wechselstube in Euro-Beträge gewechselt wurden, in das Finanzsystem einzuschleusen, müssen diese bei einem Verpflichteten des FM-GwG einbezahlt werden (siehe bereits oben unter „Finanzsektor/Guthaben bei Kredit- und Finanzinstituten“).

**(b) Risikobewusstsein:**

Siehe dazu bereits oben zu TF.

**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Insbesondere höhere Geldbeträge stellen bei der Einzahlung einen Risikofaktor für erhöhtes Risiko dar und ist in solchen Fällen die Mittelherkunft besonders genau zu prüfen. Einen risikomindernden Faktor bildet der Umstand, dass Wechselstuben in Österreich eine Konzession der FMA als KI benötigen und somit vollumfänglich zur Einhaltung der Sorgfalts- und Meldepflichten des FM-GwG verpflichtet sind.

**Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine hohe Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von Wechselstuben, für die Zwecke der Geldwäscherei missbraucht zu werden, mit mittel bis hoch einzustufen ist.**

**Risikomindernde Maßnahmen**

Wechselstuben sind als KI Verpflichtete des FM-GwG und daher von den Aufsichtsmaßnahmen der FMA erfasst. In diesem Zusammenhang führt die FMA auch Vor-Ort-Maßnahmen direkt bei Wechselstuben durch.

**Gesamtrisiko**

**Zusammenfassend ist das Risiko sowohl für TF als auf für GW als mittel einzustufen.**

**Empfehlungen**

Weitere verstärkte Zusammenarbeit zwischen den Behörden und den Stakeholdern, um sowohl auf aktuelle Muster und Trends hinzuweisen als auch die Erfahrungen im Rahmen der Weiterentwicklung der entsprechenden rechtlichen Grundlagen zu berücksichtigen.



## Finanzsektor/Elektronisches Geld (E-Geld)

### Allgemeine Informationen

Zur Ausgabe von E-Geld sind nur E-Geldemittenten berechtigt. Zu diesen zählen vor allem KI und E-Geldinstitute (Konzession der FMA). E-Geldsysteme können auch als regionale Währungen, Kundenbindungs- und Bonuspunktesysteme und Karten für Filialnetze oder Unternehmensgruppen bestehen. Handelt es sich bei diesen Systemen um sog. „begrenzte“ Netze, besteht für den Emittenten keine Verpflichtung für eine Konzessionierung durch die FMA.

### Bedrohung

#### **Terrorismusfinanzierung:**

In den zusammengefassten Szenarien der SNRA wurde die Bedrohung, dass E-Geld für terroristische Aktivitäten missbraucht wird, mit einem hohen Risiko eingestuft.

Für Terroristen oder deren Unterstützer können E-Geldprodukte insbes. dann Vorteile gegenüber Bargeld darstellen, wenn bestimmte Aktivitäten online ausgeführt werden sollen (z.B. Hotelbuchungen oder Reservierung von Mietautos). Risikomindernd wirkt sich in diesem Bereich aus, dass anonyme E-Geldprodukte in Österreich seit 01.01.2020 nicht mehr ausgegeben werden können. Einen zusätzlichen risikomindernden Faktor bildet die Nachverfolgbarkeit der Zahlungen mit E-Geldprodukten.

#### **Conclusio:**

**Zusammenfassend ist die Bedrohung mit mittel bis hoch einzustufen.**

#### **Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Bedrohung mit einem hohen Risiko eingestuft.

In den meisten Fällen können E-Geldprodukte nur mit bestimmten (z.T. verhältnismäßig niedrigen) Beträgen beladen werden, da die Emittenten derartiger Produkte von sich aus bestimmte Betragsgrenzen vorsehen.

#### **Conclusio:**

**Zusammenfassend ist die Bedrohung mit mittel einzustufen.**

### Verletzbarkeit

#### **Terrorismusfinanzierung:**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von E-Geld im Hinblick auf den Missbrauch für die Zwecke der Terrorismusfinanzierung mit hoch eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden.

#### **(a) Risikopotential:**

Zwar sind in Österreich nur eine geringe Anzahl an E-Geldemittenten im Wege der Niederlassungsfreiheit tätig, jedoch dürfen 226 E-Geldemittenten aus anderen Mitgliedstaaten ihre Produkte in Österreich im Wege der Dienstleistungsfreiheit anbieten. Letztere werden hinsichtlich der Prävention von GW/TF nicht von der FMA, sondern von der jeweils zuständigen Aufsichtsbehörde im Herkunftsmitgliedstaat beaufsichtigt.

#### **(b) Risikobewusstsein:**

Aufgrund der mit Ende des Kalenderjahres 2019 in Österreich ausgelaufenen Möglichkeit auch anonymen E-Geldprodukte auszugeben, wurde die Attraktivität, E-Geldprodukte für Zwecke der Terrorismusfinanzierung zu verwenden, weiter verringert.



**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Als Verpflichtete des FM-GwG haben E-Geldemittenten die diesbezüglichen Sorgfalts- und Meldepflichten vollumfänglich anzuwenden und werden von der FMA beaufsichtigt.

**Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine hohe Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von E-Geld, für die Zwecke der Terrorismusfinanzierung missbraucht zu werden, mit mittel einzustufen ist.**

**Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von E-Geld im Hinblick auf den Missbrauch für die Zwecke der Geldwäscherei mit mittel bis hoch eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden.

**(a) Risikopotential:**

Siehe dazu bereits oben zu TF.

**(b) Risikobewusstsein:**

Siehe dazu bereits oben zu TF.

**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Siehe dazu bereits oben zu TF.

**Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine hohe Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von E-Geld, für die Zwecke der Geldwäscherei missbraucht zu werden, mit mittel einzustufen ist.**

**Risikomindernde Maßnahmen**

E-Geldemittenten sind als Verpflichtete des FM-GwG von den Aufsichtsmaßnahmen der FMA vollumfänglich erfasst.

**Gesamtrisiko**

**Zusammenfassend ist das Risiko sowohl für TF als auch für GW als mittel einzustufen.**

**Empfehlungen**

Weitere verstärkte Zusammenarbeit zwischen den Behörden und den Stakeholdern, um sowohl auf aktuelle Muster und Trends hinzuweisen als auch die Erfahrungen im Rahmen der Weiterentwicklung der entsprechenden rechtlichen Grundlagen zu berücksichtigen.

**Finanzsektor/Zahlungsdienste**

**Allgemeine Informationen**

Zahlungsdienstleister und E-Geld-Emittenten mit Sitz in einem anderen Mitgliedstaat, die in Österreich Tätigkeiten über Dienstleister, etwa Agenten iSd § 4 Z 35 ZaDiG 2018, erbringen, unterliegen mit diesen Tätigkeiten gem. § 23 Abs. 7 FM-GwG dem Anwendungsbereich des FM-GwG. Um die Einhaltung der Vorschriften zur Prävention von GW/TF zu gewährleisten

und die Aufsicht durch die FMA zu erleichtern, haben diese Institute bei Erfüllung der Voraussetzungen der DelVO (EU) 2018/1108 der Kommission der FMA eine zentrale Kontaktstelle zu benennen. Besonders hervorzuheben ist im Rahmen der Tätigkeit durch Zahlungsdienstleister das Produkt des kontoungebundenen Bargeldtransfers.

### **Bedrohung**

#### **Terrorismusfinanzierung:**

In den zusammengefassten Szenarien der SNRA wurde die Bedrohung, dass Zahlungsdienste für terroristische Aktivitäten missbraucht werden, mit einem hohen Risiko eingestuft.

Terroristen oder deren Unterstützer können Zahlungsdienste nutzen, um Geldmittel zu transferieren und um Vermögenswerte für terroristische Aktivitäten zu erhalten/versenden. Insbesondere neue Zahlungsmethoden können dabei genutzt werden (wie z.B. über Mobiltelefone, Prepaid-Karten oder Online-Zahlungen).

#### **Conclusio:**

**Zusammenfassend ist die Bedrohung mit hoch einzustufen.**

#### **Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Bedrohung mit einem hohen Risiko eingestuft.

Zahlungsdienste können für Zwecke der Geldwäscherei, insbesondere im Rahmen der Verwendung von Geldkurieren, missbraucht werden. Dabei greifen kriminelle Organisationen auf Geldkuriere zurück, um inkriminierte Gelder in andere Jurisdiktionen zu transferieren, ohne dabei die tatsächlichen Identitäten der im Hintergrund agierenden Personen offenzulegen.

#### **Conclusio:**

**Zusammenfassend ist die Bedrohung mit hoch einzustufen.**

### **Verletzbarkeit**

#### **Terrorismusfinanzierung:**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von Zahlungsdiensten im Hinblick auf den Missbrauch für die Zwecke der Terrorismusfinanzierung mit hoch eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden.

#### **(a) Risikopotential:**

Zahlungen, die durch Zahlungsdienstleister durchgeführt werden, sind zwar nicht anonym, jedoch können relativ einfach grenzüberschreitende Transaktionen mit Hochrisiko-Kunden oder Hochrisiko-Drittstaaten durchgeführt werden.

#### **(b) Risikobewusstsein:**

Es besteht ein erhöhtes Risiko, dass österreichische Zahlungsdienstleister für Zwecke der Terrorismusfinanzierung missbraucht werden.

#### **(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Zahlungsinstitute haben als Verpflichtete des FM-GwG die diesbezüglichen Sorgfalts- und Meldepflichten vollumfänglich einzuhalten. Eine der wesentlichsten Sorgfaltspflichten stellt im Zusammenhang mit Zahlungsdiensten das Identifizieren des Kunden sowie eines ggf. vorhandenen Treuhänders dar. Daneben stellt insbesondere auch die entsprechende

Schulung und Zurverfügungstellung der notwendigen (technischen) Infrastruktur an Agenten eine wesentliche Maßnahme dar.

**Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine hohe Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von Zahlungsdiensten, für die Zwecke der Terrorismusfinanzierung missbraucht zu werden, mit hoch einzustufen ist.**

**Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von Zahlungsdiensten im Hinblick auf den Missbrauch für die Zwecke der Geldwäscherei mit hoch eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden.

**(a) Risikopotential:**

Aus den durch die FMA erhobenen Informationen und (Transaktions-)Daten ergeben sich keine Hinweise für eine besondere Verletzbarkeit des österreichischen Finanzmarktes. Einen risikoerhöhenden Faktor stellt der Umstand dar, dass nicht immer offengelegt wird und nicht immer erkennbar ist, wenn Zahlungsdienste für andere Personen als den direkten Kunden in Anspruch genommen werden.

**(b) Risikobewusstsein:**

Siehe dazu bereits oben unter (a).

**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Siehe dazu bereits oben zu TF.

**Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine mittlere Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von Zahlungsdiensten, für die Zwecke der Geldwäscherei missbraucht zu werden, mit hoch einzustufen ist.**

**Risikomindernde Maßnahmen**

Von der FMA werden thematische Schwerpunkte im Rahmen ihrer Vor-Ort-Maßnahmen gesetzt. Um die Anwendung der Strategien und Verfahren zur Prävention von GW/TF auch bei Agenten sicherzustellen, führt die FMA Vor-Ort-Maßnahmen gemeinsam bei einem Zahlungsinstitut und dessen Agenten durch. Im Rahmen der jährlich durch die FMA durchgeführte Risikoanalyse erfolgt eine Bewertung des Geschäftsmodells jedes Zahlungsinstitutes. Auf diese Weise ist gewährleistet, dass Zahlungsinstitute mit einem höheren Risiko einer erhöhten Aufsichtsintensität unterliegen.

**Gesamtrisiko**

**Zusammenfassend ist das Risiko sowohl für TF als auch für GW als hoch einzustufen.**

**Empfehlungen**

Weitere verstärkte Zusammenarbeit zwischen den Behörden und den Stakeholdern, um sowohl auf aktuelle Muster und Trends hinzuweisen als auch die Erfahrungen im Rahmen der Weiterentwicklung der entsprechenden rechtlichen Grundlagen zu berücksichtigen.

## Finanzsektor/Virtuelle Währungen

### Allgemeine Informationen

Insbesondere der hohe Grad an möglicher Anonymität bei der Verwendung von virtuellen Währungen macht diese für den Missbrauch für Zwecke von GW/TF attraktiv (im Zusammenhang mit gewissen virtuellen Währungen wird von sog. „Pseudonymität“ gesprochen). Zwar stellt die nunmehrige Regulierung von virtuellen Währungen im Bereich der Prävention von GW/TF einen risikomindernden Faktor dar, doch haben sich auch neue Methoden (z.B. Nutzung sog. „Mixer“ oder „Tumbler“) und neue Arten von virtuellen Währungen entwickelt, die die Anonymität wieder erhöhen (sog. *Anonymity Enhanced Currencies; Privacy Coins*). Die Transaktionsabwicklung erfolgt bei virtuellen Währungen grundsätzlich außerhalb der klassischen Finanzdienstleistungssysteme. Eine Nachverfolgung ist daher durch die von KI/FI verwendeten und bereits bekannten Systeme nicht möglich, sondern bedarf es spezifischer (neuer) Überwachungssysteme. Außerdem beschränken sich Transaktionen mit virtuellen Währungen nur selten auf eine Jurisdiktion. Vielmehr können damit relativ unkompliziert und schnell weitverzweigte grenzüberschreitende Transaktionen durchgeführt werden.

### Bedrohung

#### **Terrorismusfinanzierung:**

In den zusammengefassten Szenarien der SNRA wurde die Bedrohung, dass virtuelle Währungen für terroristische Aktivitäten missbraucht werden, mit einem hohen Risiko eingestuft.

Der hohe Grad an Anonymität, der bei der Verwendung von virtuellen Währungen möglich ist, führt dazu, dass Terroristen und deren Unterstützer diesen Bereich für die Finanzierung von terroristischen Aktivitäten missbrauchen können. Wie sich aus Analysen ergibt, rufen Terroristen und terroristische Gruppierungen vermehrt dazu auf, für deren Unterstützung auf Bitcoin und andere virtuelle Währungen zurückzugreifen.

#### **Conclusio:**

**Zusammenfassend ist die Bedrohung mit hoch einzustufen.**

#### **Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Bedrohung mit einem hohen Risiko eingestuft.

Auch im Bereich der Geldwäscherei stellt der hohe Grad an Anonymität bei der Verwendung von virtuellen Währungen einen Faktor für ein erhöhtes Risiko dar. Insbesondere im Bereich des *Darknets* kommt es häufig zu Zahlungen mit Bitcoin oder anderen – mit einem höheren Grad an Anonymität ausgestatteten – virtuellen Währungen. Darüber hinaus wird von kriminellen Gruppen der Tausch und Rücktausch von inkriminierten Geldern in/von virtuellen Währungen genutzt, um diese Gelder zu waschen.

#### **Conclusio:**

**Zusammenfassend ist die Bedrohung mit hoch einzustufen.**

### Verletzbarkeit

#### **Terrorismusfinanzierung:**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von virtuellen Währungen im Hinblick auf den Missbrauch für die Zwecke der Terrorismusfinanzierung mit

hoch bis sehr hoch eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden.

**(a) Risikopotential:**

Aufgrund den der FMA vorliegenden Informationen und Daten ist von sehr unterschiedlichen Strategien, Kontrollen und Verfahren bei den einzelnen Dienstleistern und deren unterschiedlichen Geschäftsmodellen auszugehen.

**(b) Risikobewusstsein:**

Aufgrund den der FMA vorliegenden Informationen und Daten ist von einem sehr unterschiedlichen Verständnis und Risikobewusstsein bei den einzelnen Dienstleistern und deren unterschiedlichen Geschäftsmodellen auszugehen.

**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Als Verpflichtete des FM-GwG haben Dienstleister in Bezug auf virtuelle Währungen seit 10. Jänner 2020 die Sorgfalts- und Meldepflichten des FM-GwG und der Geldtransfer-VO vollumfänglich anzuwenden. Vor Aufnahme ihrer Tätigkeit haben sich diese Dienstleister bei der FMA zu registrieren.

**Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine hohe bis sehr hohe Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von virtuellen Währungen, für die Zwecke der Terrorismusfinanzierung missbraucht zu werden, mit hoch einzustufen ist.**

**Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von virtuellen Währungen im Hinblick auf den Missbrauch für die Zwecke der Geldwäscherei mit hoch bis sehr hoch eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden.

**(a) Risikopotential:**

Siehe dazu bereits oben zu TF.

**(b) Risikobewusstsein:**

Siehe dazu bereits oben zu TF.

**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Siehe dazu bereits oben zu TF.

**Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine hohe bis sehr hohe Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von virtuellen Währungen, für die Zwecke der Geldwäscherei missbraucht zu werden, mit hoch einzustufen ist.**

**Risikomindernde Maßnahmen**

Da es sich in Österreich bei virtuellen Währungen um einen gänzlich neuen Kreis an Verpflichteten zur Einhaltung der Sorgfalts- und Meldepflichten handelt und wegen des beschriebenen GW/TF-Risikos, steht dieser Sektor im Fokus der Aufsicht durch die FMA. Im Jahr 2020 wurden von Seiten der FMA bereits vier Vor-Ort-Maßnahmen zur Überprüfung der Einhaltung der Bestimmungen des FM-GwG und der Geldtransfer-VO durchgeführt. Vor

Beginn der Erbringung von Dienstleistungen in Bezug auf virtuelle Währungen haben sich diese Dienstleister bei der FMA zu registrieren (2020 wurden 16 Dienstleister registriert). Verfügt die FMA im Zuge des Registrierungsverfahrens aufgrund der Angaben und Unterlagen des Dienstleisters über konkrete Anhaltspunkte, dass die Bestimmungen des FM-GwG nicht erfüllt werden können oder hat die FMA Zweifel an der persönlichen Zuverlässigkeit des/der Geschäftsführer und des/der wirtschaftlichen Eigentümer des Dienstleisters oder der natürlichen Person, die als Dienstleister tätig werden möchte, hat die FMA die Registrierung zu versagen.

#### **Gesamtrisiko**

**Zusammenfassend ist das Risiko sowohl für TF als auch für GW als hoch einzustufen.**

#### **Empfehlungen**

Weitere verstärkte Zusammenarbeit zwischen den Behörden und den Stakeholdern, um sowohl auf aktuelle Muster und Trends hinzuweisen als auch die Erfahrungen im Rahmen der Weiterentwicklung der entsprechenden rechtlichen Grundlagen zu berücksichtigen.

### **Finanzsektor/„Back-To-Back“ Geschäftsmodelle (Treuhandskredite)**

#### **Allgemeine Informationen**

Im Rahmen von sog. „Back-To-Back“ Geschäftsmodellen (auch Treuhandskredite genannt) vergeben österreichische KI/FI bar besicherte Kredite im Auftrag eines Treuhänders an einen Kreditnehmer. In den meisten Fällen handelt es sich beim Treugeber um ein anderes KI/FI aus einem Drittland. Die Kredite an den Kreditnehmer (Schuldner) werden dabei im Namen des österreichischen KI/FI aber auf Rechnung des Treugebers vergeben. Beim Kreditnehmer (Schuldner) handelt es sich in vielen Fällen um Gesellschaften in Offshore-Gebieten (die oftmals keine operativen Tätigkeiten ausüben).

Grundsätzlich werden für „Back-To-Back“ Geschäftsmodelle die folgenden Geschäftsbeziehungen eingegangen:

- 1) Einlagengeschäft: Der Treugeber tätigt bei einem österr. KI/FI eine Bareinlage.
- 2) Besicherungsgeschäft (Auftragsverhältnis): Im Rahmen eines Treuhandauftrages beauftragt der Treugeber das österreichische KI/FI, Kreditmittel im eigenen Namen, aber auf Rechnung des Treugebers an einen vom Treugeber namhaft gemachten Kreditnehmer zu vergeben. Die Bareinlage des Treugebers wird von diesem zur Sicherstellung an das österreichische KI/FI verpfändet.
- 3) Kreditgeschäft: Das österreichische KI/FI vergibt im eigenen Namen, aber auf Rechnung des Treugebers den Kredit an den Kreditnehmer (Schuldner).

Für die Abwicklung dieses Geschäftsmodells eröffnet das österreichische KI/FI einerseits ein Konto für die Bareinlage des Treugebers und andererseits ein Konto für den Kreditnehmer, auf das der Kredit zugezählt wird.

## Bedrohung

### **Terrorismusfinanzierung:**

Aus der derzeitigen Informations- und Datenlage ergeben sich keine konkreten Hinweise auf eine Bedrohungslage, wonach „Back-To-Back“ Geschäftsmodelle von Terroristen oder terroristischen Gruppierungen für deren Aktivitäten missbraucht werden.

### **Conclusio:**

**Zusammenfassend ist die Bedrohung mit niedrig einzustufen.**

### **Geldwäscherei:**

Insbesondere die Verwendung von Barmitteln für die Besicherung von Krediten stellt einen risikoerhöhenden Faktor für den Missbrauch von „Back-To-Back“ Geschäftsmodellen für Zwecke der Geldwäscherei dar. Einen weiteren risikoerhöhenden Faktor stellt in diesem Zusammenhang der Umstand dar, dass die Kredite nicht aufgrund von geschäftspolitischen Entscheidungen des kreditgewährenden Instituts, sondern aufgrund des Treuhandauftrages des Treuhänders vergeben werden. Durch „Back-To-Back“ Geschäftsmodelle werden Kredite nicht direkt von einem (ausländischen) KI/FI an einen (in den meisten Fällen ausländischen) Kreditnehmer vergeben, sondern über ein (österreichisches) KI/FI. Die Aufnahme von zusätzlichen Intermediären bei der Abwicklung von Kreditgeschäften kann deren Transparenz verringern.

### **Conclusio:**

**Zusammenfassend ist die Bedrohung mit hoch einzustufen.**

## Verletzbarkeit

### **Terrorismusfinanzierung:**

Aus der Aufsichtspraxis der FMA und den vorliegenden Daten und Informationen ergibt sich, dass es im Rahmen von „Back-To-Back“ Geschäftsmodellen derzeit zu keiner besonderen Verletzbarkeit des österreichischen Finanzmarktes, für Zwecke der Terrorismusfinanzierung missbraucht zu werden, kommt.

### **Conclusio:**

**Die dargelegten Rahmenbedingungen führen dazu, dass die Verletzbarkeit im Zusammenhang mit „Back-To-Back“ Geschäftsmodellen, für die Zwecke der Terrorismusfinanzierung missbraucht zu werden, mit niedrig einzustufen ist.**

### **Geldwäscherei:**

#### **(a) Risikopotential:**

Es gibt derzeit (Stand Ende 2020) nur einen geringen Anteil an österreichischen KI/FI, die „Back-To-Back“ Geschäftsmodelle anbieten. So reduzierte sich die Anzahl der KI, welche „Back-To-Back“ Modelle im Rahmen von Aushaftungen und Krediten bzw. von als Sicherheit dienenden Einlagen im Bestand hatten, nicht zuletzt aufgrund der hohen Aufsichtsintensität der FMA, von fünf KI im Jahr 2015 mit einem durchschnittlichen Anteil von 30,6 % der Aushaftungen bzw. Einlagen am Gesamtkredit- bzw. -einlagenportfolio auf zwei KI mit einem durchschnittlichen Anteil von 2,5 % der Aushaftungen bzw. Einlagen am Gesamtkredit- bzw. -einlagenportfolio.

#### **(b) Risikobewusstsein:**

Die FMA setzte im Rahmen ihrer Vor-Ort-Prüftätigkeit aufgrund des erhöhten Risikos von Geldwäscherei im Bereich der „Back-To-Back“ Geschäftsmodelle einen Schwerpunkt auf die Überprüfung der Einhaltung der Sorgfaltspflichten zur Prävention von GW/TF.

**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Bei „Back-To-Back“ Geschäftsmodellen müssen KI/FI jedenfalls erhöhte Sorgfaltspflichten anwenden. Aufgrund des hohen Risikos, in diesem Bereich für Geldwäscherei missbraucht zu werden, und der Aufsichtstätigkeit der FMA haben KI/FI größtenteils derartige Geschäftsmodelle abgebaut und werden diese auch nur mehr in wenigen Fällen angeboten.

**Conclusio:**

**Die dargelegten Rahmenbedingungen führen dazu, dass die Verletzbarkeit, in Zusammenhang mit „Back-To-Back“ Geschäftsmodellen für die Zwecke der Geldwäscherei missbraucht zu werden, mit hoch einzustufen ist.**

**Risikomindernde Maßnahmen**

Aufgrund des hohen GW/TF-Risikos im Bereich der „Back-To-Back“ Geschäftsmodelle stand dieser Bereich im Fokus der Aufsicht durch die FMA. Dies spiegelte sich insbesondere durch thematische Schwerpunkte im Rahmen von Vor-Ort-Prüfungen bei jenen KI/FI wider, die derartige Geschäftsmodelle anboten oder anbieten.

**Gesamtrisiko**

**Zusammenfassend ist das Risiko für TF als niedrig und für GW als hoch einzustufen.**

**Empfehlungen**

Weitere verstärkte Zusammenarbeit zwischen den Behörden und den Stakeholdern, um sowohl auf aktuelle Muster und Trends hinzuweisen als auch die Erfahrungen im Rahmen der Weiterentwicklung der entsprechenden rechtlichen Grundlagen zu berücksichtigen.

**Finanzsektor/Lebensversicherung**

**Allgemeine Informationen**

Neben der klassischen Funktion einer Lebensversicherung (Absicherung von Risiken) weisen diese auch einen Anspar- bzw. einen Finanzanlagecharakter auf und können somit, wie andere Finanzprodukte auch, für Zwecke der GW/TF missbraucht werden. Das Lebensversicherungsgeschäft stellt im Vergleich zu anderen Finanzdienstleistungen nur einen relativ geringen Anteil am österr. Finanzmarkt dar. Einige große österr. Versicherungsgruppen sind auch auf ausländischen Märkten (insbes. CESEE) aktiv.

**Bedrohung**

**Terrorismusfinanzierung:**

In den zusammengefassten Szenarien der SNRA wurde die Bedrohung, dass Lebensversicherungen für terroristische Aktivitäten missbraucht werden, mit einem mittleren Risiko eingestuft.

Aus der derzeitigen Informations- und Datenlage ergeben sich keine konkreten Hinweise auf eine besondere Bedrohungslage. Vor allem die Notwendigkeit von sehr spezifischem Know-how macht die Nutzung von Lebensversicherungen für den Bereich Terrorismusfinanzierung wenig attraktiv.

**Conclusio:**

**Zusammenfassend ist die Bedrohung mit niedrig einzustufen.**



**Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Bedrohung mit einem mittleren Risiko eingestuft.

Lebensversicherungen sind einem gezielten Missbrauch für Zwecke der Geldwäscherei zugänglich. Dies liegt in erster Linie an ihrer vorzeitigen Kündbarkeit und der damit verbundenen Rückabwicklung und Auszahlung des einbezahlten Betrages. Jedoch sehen Lebensversicherungsverträge im Falle der vorzeitigen Kündigung in der Regel für den Versicherungsnehmer sehr ungünstige Rückkaufswerte vor. Einen weiteren Risikofaktor iZm Lebensversicherungen stellt die Möglichkeit dar, aufrechte Lebensversicherungsverträge auf dem Sekundärmarkt (unter strengen Bedingungen) zu verkaufen. Dies hat für den Versicherungsnehmer den Vorteil, dass der Lebensversicherungsvertrag nicht mehr zwingend zu ungünstigen Bedingungen gekündigt werden muss. Im Allgemeinen kann festgehalten werden, dass sich aus der derzeitigen Informations- und Datenlage keine konkreten Hinweise auf eine erhöhte Bedrohungslage, wonach Lebensversicherungen zur Geldwäscherei genutzt werden, ergeben.

**Conclusio:**

**Zusammenfassend ist die Bedrohung mit niedrig einzustufen.**

**Verletzbarkeit****Terrorismusfinanzierung:**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von Lebensversicherungen im Hinblick auf den Missbrauch für die Zwecke der Terrorismusfinanzierung mit niedrig bis mittel eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden.

Aus der Aufsichtspraxis der FMA und den vorliegenden Daten und Informationen ergibt sich, dass Dienstleistungen und Produkte im Bereich der Lebensversicherung derzeit zu keiner besonderen Verletzbarkeit des österreichischen Finanzmarktes, für Zwecke der Terrorismusfinanzierung missbraucht zu werden, führen.

**Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine niedrige bis mittlere Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von Lebensversicherungen, für die Zwecke der Terrorismusfinanzierung missbraucht zu werden, mit niedrig einzustufen ist.**

**Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von Lebensversicherungen im Hinblick auf den Missbrauch für die Zwecke der Geldwäscherei mit niedrig bis mittel eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden.

**(a) Risikopotential:**

In Österreich sind Lebensversicherungen nach wie vor beliebte Anlageprodukte. Den allgemein anerkannten Typologien folgend, stellen Einmalprämienpolizzen (insbesondere iZm hohen Barerlägen) ein erhöhtes GW/TF-Risiko dar.

**(b) Risikobewusstsein:**

Da der Versicherungsmarkt in Österreich überwiegend national geprägt ist, handelt es sich bei dem Großteil der Versicherungsnehmer um natürliche Personen mit Wohnsitz in Österreich.

**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Gemäß FM-GwG haben Versicherungsunternehmen, die Lebensversicherungen anbieten, vollumfänglich die GW/TF-Sorgfaltspflichten einzuhalten. Darüber hinaus sieht das FM-GwG auch vor, dass Versicherungszahlungen an Begünstigte erst vorgenommen werden dürfen, wenn diese entsprechend den Vorgaben des FM-GwG identifiziert wurden.

**Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine niedrige bis mittlere Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von Lebensversicherungen, für die Zwecke der Geldwäscherei missbraucht zu werden, mit niedrig einzustufen ist.**

**Risikomindernde Maßnahmen**

Aufgrund der relativ geringen Zahl an Versicherungsunternehmen, die das Lebensversicherungsgeschäft betreiben und die diesbezüglichen Bestimmungen zur Prävention von GW/TF anzuwenden haben sowie der mit der Beschränkung auf den Lebensversicherungsbereich einhergehenden Homogenität der Risikomerkmale im Sektor, ist durch die derzeitige Aufsichtspraxis der FMA, insbesondere hinsichtlich der Frequenz der Vor-Ort-Maßnahmen, eine umfassende Abdeckung des Versicherungssektors gewährleistet.

**Gesamtrisiko**

**Zusammenfassend ist das Risiko sowohl für TF als auch für GW als niedrig einzustufen.**

**Empfehlungen**

Weitere verstärkte Zusammenarbeit zwischen den Behörden und den Stakeholdern, um sowohl auf aktuelle Muster und Trends hinzuweisen als auch die Erfahrungen im Rahmen der Weiterentwicklung der entsprechenden rechtlichen Grundlagen zu berücksichtigen.

**Finanzsektor/Safe-Vermietung**

**Allgemeine Informationen**

Bei der Zurverfügungstellung (Vermietung) von Wertfächern (Safes) werden grundsätzlich Schließfächer, typischerweise unter Mitverschluss (Doppelsperre) durch den Vermieter, den dabei besondere Sicherungspflichten treffen, gegen Entgelt zur Verfügung gestellt.

**Bedrohung**

**Terrorismusfinanzierung:**

Aus der derzeitigen Informations- und Datenlage ergeben sich keine konkreten Hinweise auf eine Bedrohungslage, wonach die Erbringung von Schließfachverwaltungsdiensten von Terroristen oder terroristischen Gruppierungen für deren Aktivitäten missbraucht werden.

**Conclusio:**

**Zusammenfassend ist die Bedrohung mit niedrig einzustufen.**

**Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Bedrohung mit einem hohen Risiko eingestuft.

Schließfächer (Safes) können dazu verwendet werden, inkriminierte Vermögenswerte zu verstecken, um diese in Folge in einzelnen (kleineren) Tranchen in das Finanzsystem zu integrieren. Eine Umwandlung dieser Vermögenswerte in nicht inkriminierte Vermögenswerte ist damit aber nicht möglich.

**Conclusio:**

**Zusammenfassend ist die Bedrohung mit mittel einzustufen.**

**Verletzbarkeit****Terrorismusfinanzierung:**

Aus der Aufsichtspraxis der FMA und den vorliegenden Daten und Informationen ergibt sich, dass Dienstleistungen und Produkte im Bereich von Schließfachverwaltungsdiensten derzeit zu keiner besonderen Verletzbarkeit des österreichischen Finanzmarktes, für Zwecke der Terrorismusfinanzierung missbraucht zu werden, führen.

**Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die keine Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von Dienstleistungen und Produkten im Bereich von Schließfachverwaltungsdiensten, für die Zwecke der Terrorismusfinanzierung missbraucht zu werden, mit niedrig einzustufen ist.**

**Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von Schließfachverwaltungsdiensten im Hinblick auf den Missbrauch für die Zwecke der Geldwäscherei mit mittel bis hoch eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden.

**(a) Risikopotential:**

Beim überwiegenden Teil der angebotenen Schließfachverwaltungsdiensten in Österreich handelt es sich um die klassische Form der Bankschließfachvermietung durch konzessionierte KI.

**(b) Risikobewusstsein:**

Schließfachverwaltungsdienste durch sonstige Unternehmen stellen ein nur geringes Risiko dar, diese sind als Verpflichtete des FM-GwG ebenfalls vollumfänglich den Sorgfalts- und Meldepflichten des FM-GwG unterworfen.

**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Die Zurverfügungstellung (Vermietung) von Wertfächern (Safes) ist als Erbringung von Schließfachverwaltungsdiensten dem Geschäftsbereich von FI iSd § 1 Abs. 2 BWG zuzuordnen. Anbieter von Schließfachverwaltungsdiensten sind daher Verpflichtete des FM-GwG und haben die Sorgfalts- und Meldepflichten des FM-GwG vollumfänglich anzuwenden.

**Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine mittlere bis hohe Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die**

<b>Verletzbarkeit von Schließfachverwaltungsdiensten, für die Zwecke der Geldwäscherei missbraucht zu werden, mit mittel einzustufen ist.</b>
<b>Risikomindernde Maßnahmen</b>
Die FMA kann bei Verstößen gegen die Sorgfalts- und Meldepflichten des FM-GwG Verwaltungsstrafen verhängen. Über Anbieter von Schließfachverwaltungsdiensten, die anonyme Schließfächer (Safes) in der Vergangenheit angeboten haben, und damit gegen die Verpflichtung zur Feststellung und Überprüfung der Identität ihrer Kunden verstoßen haben, wurden von der FMA entsprechende Verwaltungsstrafen verhängt.
<b>Gesamtrisiko</b>
<b>Zusammenfassend ist das Risiko für TF als niedrig und für GW als mittel einzustufen.</b>
<b>Empfehlungen</b>
Weitere verstärkte Zusammenarbeit zwischen den Behörden und den Stakeholdern, um sowohl auf aktuelle Muster und Trends hinzuweisen als auch die Erfahrungen im Rahmen der Weiterentwicklung der entsprechenden rechtlichen Grundlagen zu berücksichtigen.

<b>Finanzsektor/Geschäftskredite</b>
<b>Allgemeine Informationen</b>
Kriminelle, Terroristen oder deren Unterstützer tilgen mit inkriminierten Vermögenswerten Geschäftskredite.
<b>Bedrohung</b>
<b>Terrorismusfinanzierung:</b> In den zusammengefassten Szenarien der SNRA wurde die Bedrohung, dass Geschäftskredite für terroristische Aktivitäten missbraucht werden, mit einem niedrigen Risiko eingestuft.  Aus den der FMA vorliegenden Informationen und Daten ergeben sich keine konkreten Hinweise auf eine Bedrohungslage, wonach terroristische Organisationen Geschäftskredite zur Terrorismusfinanzierung nutzen.
<b>Conclusio:</b> <b>Zusammenfassend ist die Bedrohung mit niedrig einzustufen.</b>
<b>Geldwäscherei:</b> In den zusammengefassten Szenarien der SNRA wurde die Bedrohung mit einem mittleren Risiko eingestuft. Aus den der FMA vorliegenden Informationen und Daten ergeben sich keine konkreten Hinweise auf eine Bedrohungslage, wonach Geschäftskredite zur Geldwäscherei genutzt werden.
<b>Conclusio:</b> <b>Zusammenfassend ist die Bedrohung mit mittel einzustufen.</b>

<b>Verletzbarkeit</b>
<p><b>Terrorismusfinanzierung:</b> Aus der Aufsichtspraxis der FMA und den vorliegenden Daten und Informationen ergibt sich, dass Dienstleistungen und Produkte im Bereich der Geschäftskredite derzeit zu keiner besonderen Verletzbarkeit des österreichischen Finanzmarktes, für Zwecke der Terrorismusfinanzierung missbraucht zu werden, führen.</p> <p><b>Conclusio:</b> <b>Ausgehend von den zusammengefassten Szenarien der SNRA, die eine niedrige Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von Geschäftskrediten, für die Zwecke der Terrorismusfinanzierung missbraucht zu werden, mit niedrig einzustufen ist.</b></p>
<p><b>Geldwäscherei:</b> Aus der Aufsichtspraxis der FMA und den vorliegenden Daten und Informationen ergibt sich, dass Dienstleistungen und Produkte im Bereich der Geschäftskredite derzeit zu keiner besonderen Verletzbarkeit des österreichischen Finanzmarktes, für Zwecke der Geldwäscherei missbraucht zu werden, führen.</p> <p><b>Conclusio:</b> <b>Ausgehend von den zusammengefassten Szenarien der SNRA, die eine mittlere Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von Geschäftskrediten, für die Zwecke der Geldwäscherei missbraucht zu werden, mit niedrig bis mittel einzustufen ist.</b></p>
<b>Risikomindernde Maßnahmen</b>
Der Abschluss von Kreditverträgen ist gemäß § 1 Abs. 1 Z 3 BWG Kreditinstituten vorbehalten und bedarf einer Konzession der FMA. Neben den weiteren Sorgfaltspflichten des FM-GwG haben KI gegenüber Kunden vor allem auch über ausreichend Information hinsichtlich der Mittelherkunft, etwa bei Tilgungszahlungen von Krediten oder bei vom ursprünglichen Vertrag abweichenden Tilgungszahlungen, zu verfügen. Diese Informationen sind vom KI auch entsprechend zu überprüfen.
<b>Gesamtrisiko</b>
<b>Zusammenfassend ist das Risiko sowohl für TF als auch für GW als niedrig einzustufen.</b>
<b>Empfehlungen</b>
Weitere verstärkte Zusammenarbeit zwischen den Behörden und den Stakeholdern, um sowohl auf aktuelle Muster und Trends hinzuweisen als auch die Erfahrungen im Rahmen der Weiterentwicklung der entsprechenden rechtlichen Grundlagen zu berücksichtigen.

<b>Finanzsektor/Konsumenten- bzw. Kleinkredite</b>
<b>Allgemeine Informationen</b>
Terroristen bzw. Gruppen des organisierten Verbrechens nutzen zeitlich kurz befristete Konsumenten- bzw. Kleinkredite mit hohen Zinsen, jedoch geringen Kreditbeträgen. Dies kann etwa durch die Überziehung des Kreditkartenlimits erfolgen ohne Absicht, diesen überzoge-

nen Betrag wieder zu ersetzen. Weiters können Konsumenten- bzw. Kleinkredite für Geldwäscherei genutzt werden, indem damit teure Güter (z.B. Fahrzeuge, Schmuck) gekauft werden und frühzeitig zurückgezahlt werden.

### **Bedrohung**

#### **Terrorismusfinanzierung:**

In den zusammengefassten Szenarien der SNRA wurde die Bedrohung, dass Konsumenten- bzw. Kleinkredite für terroristische Aktivitäten missbraucht werden, mit einem hohen Risiko eingestuft.

Terroristische Gruppierungen oder auch (radikalisierte) Einzelpersonen können Konsumenten- bzw. Kleinkredite insbesondere dafür nutzen, um Reisen von sog. „Foreign Terrorist Fighters“ oder für sich selbst in Krisengebiete zu finanzieren.

#### **Conclusio:**

**Zusammenfassend ist die Bedrohung mit mittel bis hoch einzustufen.**

#### **Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Bedrohung mit einem mittleren Risiko eingestuft.

Im Vergleich zu anderen Finanzprodukten bieten Konsumenten- bzw. Kleinkredite wenig Potential, um für Geldwäscherei missbraucht zu werden – insbesondere um größere Geldmengen „reinzuwaschen“.

#### **Conclusio:**

**Zusammenfassend ist die Bedrohung mit niedrig bis mittel einzustufen.**

### **Verletzbarkeit**

#### **Terrorismusfinanzierung:**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von Konsumenten- bzw. Kleinkrediten im Hinblick auf den Missbrauch für die Zwecke der Terrorismusfinanzierung mit hoch eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden.

#### **(a) Risikopotential:**

Die Transaktionsvolumina sind in der Regel zwar niedrig und Kontrollsysteme bei den KI sind vorhanden. Dies reduziert jedoch nicht signifikant das Risiko der Verletzbarkeit für den österreichischen Finanzmarkt.

#### **(b) Risikobewusstsein:**

Risiken können sich insbesondere dort ergeben, wo wenig Bewusstsein für die Einstellung der Transaktionsmonitoringsysteme gegeben ist bzw. wo Verpflichtete verstärkt auf Möglichkeiten der Fernidentifizierung zurückgreifen und dies von Verpflichteten nicht adäquat berücksichtigt wird.

#### **(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

KI haben neben den weiteren Sorgfaltspflichten des § 6 FM-GwG insbesondere auch über ausreichend KYC-Informationen des Kunden zu verfügen. Außerdem haben sie entsprechend eingestellte Transaktionsmonitoringsysteme zu installieren.

<p><b>Conclusio:</b>  Ausgehend von den zusammengefassten Szenarien der SNRA, die eine hohe Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von Konsumenten- bzw. Kleinkrediten, für die Zwecke der Terrorismusfinanzierung missbraucht zu werden, mit mittel bis hoch einzustufen ist.</p>
<p><b>Geldwäscherei:</b>  In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von Konsumenten- bzw. Kleinkrediten im Hinblick auf den Missbrauch für die Zwecke der Geldwäscherei mit mittel eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden.</p> <p><b>(a) Risikopotential:</b>  Aufgrund der in der Regel niedrigen Beträge und des verhältnismäßig geringen Anteils an Konsumenten- bzw. Kleinkrediten ist die Risikoexposition dieses Bereiches als niedrig anzusehen.</p> <p><b>(b) Risikobewusstsein:</b>  Siehe dazu bereits oben zu TF.</p> <p><b>(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:</b>  KI haben neben den weiteren Sorgfaltspflichten des § 6 FM- GwG insbesondere auch über ausreichend Information hinsichtlich der Mittelherkunft des Kunden, etwa bei Tilgungszahlungen von Krediten, zu verfügen. Außerdem haben sie entsprechend eingestellte Transaktionsmonitoringsysteme zu installieren.</p> <p><b>Conclusio:</b>  Ausgehend von den zusammengefassten Szenarien der SNRA, die eine hohe Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von Konsumenten- bzw. Kleinkrediten, für die Zwecke der Geldwäscherei missbraucht zu werden, mit niedrig bis mittel einzustufen ist.</p>
<p><b>Risikomindernde Maßnahmen</b></p>
<p>Der Abschluss von Kreditverträgen ist gemäß § 1 Abs. 1 Z 3 BWG Kreditinstituten vorbehalten. Die FMA überprüft im Rahmen ihrer Vor-Ort-Prüftätigkeit schwerpunktmäßig auch die richtige Kalibrierung der Transaktionsmonitoringsysteme von Verpflichteten.</p>
<p><b>Gesamtrisiko</b></p>
<p><b>Zusammenfassend ist das Risiko für TF als mittel bis hoch und für GW als mittel einzustufen.</b></p>
<p><b>Empfehlungen</b></p>
<p>Weitere verstärkte Zusammenarbeit zwischen den Behörden und den Stakeholdern, um sowohl auf aktuelle Muster und Trends hinzuweisen als auch die Erfahrungen im Rahmen der Weiterentwicklung der entsprechenden rechtlichen Grundlagen zu berücksichtigen.</p>

## Finanzsektor/Hypothekarkredit

### Allgemeine Informationen

Hypothekarkredite werden für die Finanzierung von Immobilien verwendet, indem die zu erwerbende Immobilie als Pfand für die Kreditrückzahlung bestellt wird. Im Bereich Geldwäscherei können die Erträge aus Straftaten für Immobilieninvestments genutzt werden, indem die Erträge z.B. für Tilgungszahlungen bzw. vorzeitige Tilgung verwendet werden. Grundsätzlich besteht auch die Möglichkeit, dass Terroristen oder deren Unterstützer mittel- bis langfristige Hypothekarkredite mit hoher Summe dazu nutzen, um ihre Aktivitäten zu finanzieren.

### Bedrohung

#### **Terrorismusfinanzierung:**

In den zusammengefassten Szenarien der SNRA wurde die Bedrohung, dass Hypothekarkredite für terroristische Aktivitäten missbraucht werden, mit einem niedrigen Risiko eingestuft.

Die Nutzung von Hypothekarkrediten für terroristische Zwecke gestaltet sich insbesondere wegen der Bindung an eine Immobilie, der damit verbundenen Eintragung in das Grundbuch und der langfristigen Bindung schwierig und ist für Terroristen oder deren Unterstützer kaum zugänglich.

#### **Conclusio:**

**Zusammenfassend ist die Bedrohung mit niedrig einzustufen.**

#### **Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Bedrohung mit einem hohen Risiko eingestuft.

Hypothekarkredite können zur Geldwäscherei genutzt werden, um so höhere Beträge an inkriminierten Geldern durch den Kauf von (mehreren) Immobilien in das Finanzsystem zu schleusen. Insbesondere durch die Verwendung von gefälschten Dokumenten und Unterlagen versuchen Gruppen der organisierten Kriminalität die tatsächlichen wirtschaftlichen Eigentümer und die Herkunft der eingesetzten Mittel für den Erwerb von Immobilien zu verschleiern. Als risikomindernd ist zu berücksichtigen, dass im Bereich der Hypothekarkredite immer KI für die Abwicklung eingebunden werden müssen. Außerdem bedarf es für die vertragliche Ausgestaltung und die grundbücherliche Eintragung der Beiziehung von Notaren und Rechtsanwälten.

#### **Conclusio:**

**Zusammenfassend ist die Bedrohung mit mittel bis hoch einzustufen.**

### Verletzbarkeit

#### **Terrorismusfinanzierung:**

Aus der Aufsichtspraxis der FMA und den vorliegenden Daten und Informationen ergibt sich keine besondere Verletzbarkeit des österreichischen Finanzmarktes.

#### **Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine niedrige Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von Hypothekarkrediten, für die Zwecke der Terrorismusfinanzierung missbraucht zu werden, mit niedrig einzustufen ist.**



**Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von Guthaben bei KI/FI im Hinblick auf den Missbrauch für die Zwecke der Geldwäscherei mit mittel eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden.

**(a) Risikopotential:**

Hypothekarkredite – insbesondere von privaten Haushalten – stellen in Österreich einen wichtigen Bestandteil der Geschäftsmodelle von KI dar.

**(b) Risikobewusstsein:**

Viele kleinere Hypothekarkredite werden für die Anschaffung von Wohnraum zum Eigennutzen abgeschlossen. Dabei handelt es sich um verhältnismäßig geringe Kreditvolumina. Ein höheres Risiko stellen vor allem großvolumige – zum Teil auch rein spekulative – Immobiliengeschäfte dar.

**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

KI haben neben den weiteren Sorgfaltspflichten des § 6 FM-GwG insbesondere auch über ausreichend Information hinsichtlich der Mittelherkunft des Kunden, etwa bei Tilgungszahlungen von Krediten, zu verfügen. Außerdem haben sie entsprechend eingestellte Transaktionsmonitoringsysteme zu installieren.

**Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine mittlere Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von Hypothekarkrediten, für die Zwecke der Geldwäscherei missbraucht zu werden, mit mittel bis hoch einzustufen ist.**

**Risikomindernde Maßnahmen**

Hypothekarkredite stellen aufgrund ihres zum Teil erhöhten Risikos für Zwecke der Geldwäscherei missbraucht zu werden einen thematischen Schwerpunkt der FMA im Rahmen ihrer Vor-Ort-Prüftätigkeit dar. Unter anderem überprüft die FMA dabei im Detail, wie Kreditinstitute bei Hypothekarkrediten die Mittelherkunft überprüft und mit den KYC-Informationen plausibilisiert. Außerdem wird die adäquate Kalibrierung der Transaktionsmonitoringsysteme hinsichtlich der Rückzahlungsmodalitäten überprüft.

**Gesamtrisiko**

**Zusammenfassend ist das Risiko für TF als niedrig und für GW als mittel einzustufen.**

**Empfehlungen**

Weitere verstärkte Zusammenarbeit zwischen den Behörden und den Stakeholdern, um sowohl auf aktuelle Muster und Trends hinzuweisen als auch die Erfahrungen im Rahmen der Weiterentwicklung der entsprechenden rechtlichen Grundlagen zu berücksichtigen.

**Human- und Finanzressourcen**

Der FMA stehen 27,25 Vollbeschäftigtenäquivalente zur Verfügung. Den für das AltFG zuständigen Behörden stehen 0,1072 Vollbeschäftigtenäquivalente zur Verfügung.

# Risiko der Verletzung von Sanktionsmaßnahmen

## Risiko der Verletzung von Sanktionsmaßnahmen

### Allgemeine Informationen

Die Zuständigkeit zur Überwachung der Einhaltung von gesetzmäßigen Bestimmungen nach dem Sanktionengesetz 2010 durch das BVT ergibt sich aus der Geschäftseinteilung des Bundesministeriums für Inneres. Die bestehenden Resolutionen sowie auch Sanktionsmaßnahmen treffen mehrere Bereiche. Nicht zuletzt folgt auch die mit der Überwachung von Finanztransaktionen im Bereich der Kredit- und Finanzinstitute beauftragte Oesterreichische Nationalbank der groben Unterteilung in Terrorismus(finanzierung), Proliferation sowie länderspezifische Sanktionsmaßnahmen. Sämtliche Verstöße iSd. Sanktionengesetz 2010, die unter Vermögensbestandteile von Euro 100.000.- fallen, werden durch die Bezirksverwaltungsbehörden sowie Landespolizeidirektionen als Verwaltungsstrafverfahren geführt.

Die im BVT Referat Nachrichtendienst - Fachbereich Geldwäsche und Wirtschaftsspionage - einlangenden Verdachtsmeldungen im Hinblick auf etwaige Sanktionsbrüche oder Verstöße werden zu einem überwiegenden Teil durch die A-FIU übermittelt. Fast ausschließlich handelt es sich dabei um Geldwäscheverdachtsmeldungen von Bankinstituten. In der Regel werden einzelne Personen sowie auch Unternehmen (vorwiegend Einzelunternehmen und GesmbH) in Verbindung mit Finanztransaktionen bekanntgegeben. Zu einem weitaus geringeren Teil erfolgen Mitteilungen direkt durch das BMF sowie auch andere Organisationen wie das BMeiA und selten anonym.

Die doch deutliche Mehrheit an Verdachtsmeldungen an die A-FIU durch Bank- und Finanzinstitute wird auf den sensiblen Umgang betreffend die Meldepflichten und die daraus resultierenden oft empfindlichen Strafen gemäß Finanzmarktgeldwäschegesetz zurückgeführt.

Bei der Aufarbeitung der verschiedenen Sachverhalte erfolgt eine regelmäßige Rückmeldung an die A-FIU über den Verlauf, insbesondere sobald Erkenntnisse über Verdachtsmomente an das zuständige Gericht übermittelt werden. Aufgrund der Kompetenzhoheit der A-FIU, der die Kontaktaufnahme mit sämtlichen Kredit- und Finanzinstituten obliegt, erfolgen keine Vermögens- oder Finanzermittlungen durch den Fachbereich im Referat Nachrichtendienst.

Die oftmals schwierige Abgrenzung der Sachverhalte zwischen den Bereichen Proliferation und länderspezifischen Sanktionsmaßnahmen erschwert eine statistische Erhebung der Gesamtanzahl von Sanktionsüberwachungen und liegt derzeit nicht auf. Auch eine Anzahl der in der OeNB vermerkten Fälle ist im Fachbereich nicht bekannt.

Im BVT werden die Verdachtsmeldungen in Zusammenwirken mit der A-FIU, dem Bundeskriminalamt sowie auch der OeNB anhand der geltenden Resolutionen und Rechtsakte verarbeitet. Als Arbeitsgrundlage dienen sowohl die entsprechende UN- als auch EU Sanktionslisten. Bei entsprechender Verdachtslage erfolgt einerseits die vertiefende Zusammenarbeit

mit dem BMF sowie auch die Berichterstattung an das zuständige Gericht und gemäß der Wertgrenze von Vermögensbestandteilen an die entsprechende Bezirksverwaltungsbehörde, bzw. Landespolizeidirektion. Die Zusammenarbeit mit den genannten Behörden darf durchaus als kooperativ bezeichnet werden.

### **Bedrohung**

Eine vollständige statistische Auswertung, die auch als Grundlage zur Bewertung des Risikos von „Sanktionsbrüchen“ herangezogen werden könnte, kann demzufolge nicht ausschließlich durch das BVT beigebracht werden. Jedoch weisen die Zahlen der im Fachbereich eingemeldeten Verdachtsmeldungen betreffend Sanktionengesetz über die letzten Jahre hindurch keine signifikanten Änderungen in eine bestimmte Richtung auf und stellen im Gesamtkontext eher die Minderheit dar.

### **Empfehlungen**

Sowohl die rechtliche Beurteilung als auch die Einschätzung der Sachverhalte in Terrorismus, Proliferation und länderspezifische Sanktionsmaßnahmen gestaltet sich speziell in der operativen Fallbearbeitung als schwierig. Ein möglicher Lösungsansatz bestünde in der Etablierung eines klaren Abarbeitungsprozesses. Die Komplexität der Materie in Verbindung mit den möglichen Rechtsfolgen und der daraus resultierenden Außenwirkung macht es notwendig, neben dem entsprechenden juristischen Fachwissen auch einen fruchtbaren Informationsaustausch anzustreben.

# Risiko der Umgehung von EU-Finanzsanktionen gegen Terrorismusfinanzierung

## EU-Finanzsanktionen gegen Terrorismusfinanzierung/Finanzsektor (Kredit-, Finanz- und Zahlungsinstitute)

### Allgemeine Informationen

Sanktionsmaßnahmen gegen Terrorismusfinanzierung werden von der Europäischen Union in Form von Verordnungen verhängt. Dies sowohl in Umsetzung von Resolutionen des Sicherheitsrates der Vereinten Nationen als auch zur Erlassung EU-autonomer restriktiver Maßnahmen. Die in der Regel durch EU-Verordnungen auf Grundlage von Art. 215 AEUV erfolgten Maßnahmen gelten wie nationales Recht unmittelbar in jedem Mitgliedstaat (Art. 288 AEUV) und richten sich direkt an die jeweiligen Rechtsanwender. Somit sind etwa auch Kreditinstitute im Rahmen ihrer Geschäftstätigkeit unmittelbar daran gebunden. Im nationalen Recht bildet v.a. das SanktG 2010 die relevante rechtliche Grundlage iZm mit der Einhaltung von Sanktionsvorschriften.

Restriktive Maßnahmen werden als ein wichtiges Instrument der Gemeinsamen Außen- und Sicherheitspolitik (GASP) erachtet, die eine Änderung in der Politik oder im Handeln derjenigen bewirken sollen, gegen die sich die Maßnahmen richten, und damit die Ziele der GASP unterstützen. Finanzsanktionen befassen sich dabei im Wesentlichen mit Beschränkungen des Kapital- und Zahlungsverkehrs. Die Gründe für die Verhängung von restriktiven Maßnahmen sind unterschiedlich gelagert und folglich im Einklang mit ihrem jeweiligen Zweck zu behandeln. Die gegenständliche Analyse soll sich auf restriktive Maßnahmen gegen Terrorismusfinanzierung („gelistete“ Terroristen) beschränken.

Der klassische Anwendungsfall von Sanktionen betrifft umfassende Verpflichtungen zum Einfrieren von Geldern und wirtschaftlichen Ressourcen. Damit geht auch ein entsprechendes unmittelbares und mittelbares Bereitstellungsverbot einher. Explizit untersagt ist es, wissentlich Handlungen zu setzen, die zu einer Umgehung der restriktiven Maßnahmen führen bzw. diese begünstigen. Maßgeblich ist es sicherzustellen, dass keiner sanktionierten Person, Organisation oder Einrichtung Gelder oder wirtschaftliche Ressourcen unmittelbar oder mittelbar zur Verfügung gestellt werden, keine sanktionsrechtlich untersagten Transaktionen durchgeführt und auch keine sonstigen Leistungen erbracht werden, denen sanktionsrechtliche Maßnahmen zu Grunde liegen.

### Bedrohung

Eine Gefahr besteht insbesondere in der Umgehung von restriktiven Maßnahmen gegen Terrorismusfinanzierung. Dazu können etwa intransparente Strukturen aufgesetzt und juristische Personen missbraucht werden, indem beispielsweise komplexe Gesellschaftsstrukturen, treuhänderisches Agieren oder ähnliche, intransparente Konstruktionen (Off-Shore, Zwischenschalten von nicht unternehmerisch tätigen Gesellschaften etc) geschaffen werden, durch welche die Feststellung und Überprüfung der Identität des tatsächlichen wirtschaftlichen Eigentümers bzw. der tatsächliche wirtschaftliche Gehalt einer Transaktion (mutwillig) erschwert wird.

Abgrenzungsschwierigkeiten können sich uU bei Transaktionen ergeben, die zwar mit einer nicht sanktionierten Person, Organisation oder Einrichtung eingegangen werden sollen, die aber in einem gewissen Naheverhältnis zu einer gelisteten Person, Organisation oder Einrichtung steht. Dabei ist zu beachten und zu prüfen, ob nicht eine ebenfalls verbotene mittelbare Bereitstellung von Geldern und wirtschaftlichen Ressourcen an sanktionierte Personen, Organisationen oder Einrichtungen erfolgt. Problematisch ist etwa, wenn Treuhandverhältnisse nicht offengelegt und auch sonst nicht nach außen hin ersichtlich sind oder (verdeckte) Treuhandkonstruktionen unter Zuhilfenahme von zwischengeschalteten Off-Shore-Unternehmen geschaffen werden.

**Conclusio:**

**Aufgrund der beschriebenen Bedrohungslage besteht für den Finanzsektor ein inhärentes (mittleres bis hohes) Risiko, für die Umgehung von sanktionsrechtlichen Bestimmungen missbraucht zu werden.**

**Verletzbarkeit**

**a) Risikopotential:**

Die Ermittlung des tatsächlichen wirtschaftlichen Gehalts von Transaktionen sowie die eindeutige Feststellung der „Beneficial Owner“ sind von essenzieller Bedeutung, um potenzielle Verletzungen sanktionsrechtlicher Normen zu erkennen und hintanzuhalten. Die Implementierung einheitlicher Prozessabläufe und Dokumentationsvorgaben ist erforderlich, um hintanzuhalten, dass sanktionsrechtliche Normen verletzt oder umgangen werden.

Das Risiko besteht insbesondere bei komplexen, intransparenten Unternehmensstrukturen, bei welchen die Eigentums- bzw. Kontrollverhältnisse nur schwer offenkundig werden. Bei grenzüberschreitenden Sachverhalten können zudem insbesondere der Informationsaustausch, unterschiedliche Rechtslagen bzw. Auslegungen, fremdartige Urkunden und Dokumente etc. die Prüfung der Eigentümer- und Kontrollstruktur bzw. den wirtschaftlichen Gehalt einer Transaktion erschweren.

**(b) Risikobewusstsein:**

Es hat sich gezeigt, dass die Umsetzung von Sanktionsmaßnahmen im Finanzsektor bezüglich Vermögenswerte, die den in den jeweiligen Sanktionslisten angeführten Personen, Organisationen oder Einrichtungen zuzuordnen sind, bei Vorliegen der entsprechenden Systeme und Prozesse, weitgehend gut funktioniert. Auch die SNRA impliziert ein weitgehend funktionierendes Sanktionsscreening (und sieht Risiken v.a. bezüglich nicht gelisteter (unbekannter) Personen, die terroristische Aktivitäten ausüben).

Dem Finanzsektor wurde generell ein gutes Verständnis zu den Gefahren und Risiken in den relevanten Compliance-Bereichen von der FATF zuerkannt.<sup>1</sup>

**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Die rechtlichen Rahmenbedingungen sind vorrangig in den jeweiligen EU-Verordnungen enthalten. Verwaltungsstrafbestimmungen- und gerichtliche Strafrechtsbestimmungen sind in den §§ 11 SanktG 2010 ff normiert.

Die OeNB ist für die Kontrolle der Einhaltung sanktionsrechtlicher Maßnahmen im Bereich der Kredit-, Finanz- und Zahlungsinstitute zuständig (§ 8 Abs. 1 SanktG 2010). Dazu nimmt diese insbesondere ihre Überwachungs- und Auskunftsbefugnisse nach § 8 Abs. 2 SanktG 2010 wahr. Überwachungs- und Auskunftsbefugnisse der OeNB sind auch in § 5 DevG 2004 vorgesehen.

<sup>1</sup> FATF, MER (2016), 226.

**Human- und Finanzressourcen:**

Zur Erfüllung der durch § 8 Abs. 1 Sanktionengesetz 2010 der OeNB zugewiesenen Aufgaben im Bereich der Kredit- und Finanzinstitute gemäß § 1 BWG sowie der in § 4 Z 4 des Zahlungsdienstegesetzes 2018 – ZaDiG 2018, BGBl. I Nr. 17/2018, genannten Zahlungsinstitute ist ein Pool an Mitarbeitern aus zwei Abteilungen bedarfsabhängig zugewiesen: Die Rechtsabteilung ist für den behördlichen Teil des Sanktionenregimes zuständig, während die Abteilung für Bankenrevision Vor-Ort-Prüfungen bei Kredit-, Finanz- und Zahlungsinstituten vornimmt. EU-Finanzsanktionen gegen Terrorismusfinanzierung sind ein Teil der von der OeNB zu vollziehenden Aufgaben im Sanktionenbereich. Für das Jahr 2021 sind insgesamt 1,1 Vollbeschäftigtenäquivalente für diesen Aufgabenbereich planmäßig veranschlagt.

**Conclusio:**

**Aufgrund der beschriebenen Lage besteht ein inhärentes Risiko (mittel), dass Institute Sanktionsverstöße bzw. -umgehungen nicht erkennen.**

**Risikomindernde Maßnahmen****Maßnahmen durch Institute:**

Institute haben im Rahmen ihrer Sorgfaltspflichten sicherzustellen, dass keiner sanktionierten Person, Organisation oder Einrichtung Gelder oder wirtschaftliche Ressourcen unmittelbar oder mittelbar zur Verfügung gestellt werden und auch sonst keine sanktionsrechtlich untersagten Transaktionen durchgeführt werden. Darüber hinaus sind Melde- und Genehmigungspflichten zu beachten. Institute haben IT-Tools zur Überwachung von sanktionsrechtlichen Maßnahmen in Kreditinstituten implementiert. Mit diesen Systemen werden sowohl Transaktionen als auch der Kundenbestand auf sanktionsrechtlich relevante Sachverhalte überprüft, auf Basis der Prüfung können Transaktionen gestoppt bzw. Konten gesperrt werden. Im Rahmen der Beurteilung von Transaktionen sind die Grundlagen und der wirtschaftliche Gehalt in die Betrachtung miteinzubeziehen. Umstände des Einzelfalls sind risikobasiert zu beachten. So sind etwa die Feststellung des wirtschaftlichen Eigentümers und die Ermittlung des tatsächlichen wirtschaftlichen Gehalts einer Transaktion in diesem Zusammenhang relevant. Auch hier ist eine risikobasierte Vorgehensweise bei den Prüfungshandlungen durch das jeweilige Institut unabdingbar, um die Einhaltung der Sorgfaltspflichten zu gewährleisten. Dazu zählen neben Durchführung einer umfangreichen „Customer-Due-Diligence“ Prüfung und der Beachtung des KYC-Prinzips die Einholung zusätzlicher Informationen zu den Transaktionen, zur Herkunft der eingesetzten Mittel und zu Zweck und Art der Geschäftsbeziehung. Außerdem haben Institute bei Hochrisiko-Kunden eine intensivere, kontinuierliche Überwachung der Geschäftsbeziehung und der Transaktionen sicherzustellen und eine tourliche Aktualisierung der Kundenunterlagen durchzuführen. Die Implementierung geeigneter Prozesse und das Setzen entsprechender Maßnahmen ist nicht nur erforderlich, um sanktionsrelevante Transaktionen, sondern auch um Umgehungshandlungen zu erkennen und die Durchführung der damit verbundenen Transaktionen zu verhindern. Eine entsprechende Awareness-Bildung bei den Mitarbeitenden der Institute findet statt.

**Aufsichtsmaßnahmen:**

Die OeNB steht mit dem Finanzsektor regelmäßig in Kontakt, nimmt Auskunftsbefugnisse (§ 8 Abs. 2 SanktG 2010) wahr und wird auch iZm der Beurteilung von Sachverhalten mit etwaigen Sanktionsbezug konsultiert. Die Erteilung von Informationen bzw. Leitlinien betreffend die Einhaltung von Sanktionsmaßnahmen gilt als üblicher internationaler Standard.

Beaufsichtigte Institute erstatten der OeNB auf Basis der jeweiligen anwendbaren Rechtsgrundlagen (in der Regel die jeweiligen EU-Verordnungen) Meldungen, wobei Angaben zu eingefrorenen Geldern hervorzuheben sind. Die OeNB kann im Rahmen der gesetzlichen

Möglichkeiten Ausnahmegenehmigungen erteilen, etwa bezüglich der Freigabe von eingefrorenen Geldern.

Im Rahmen von Vor-Ort Prüfungen im Bereich von Finanzsanktionen wird evaluiert, inwieweit die im geprüften Kreditinstitut angewandten Systeme geeignet sind, die Einhaltung der devisen- und sanktionsrechtlichen Bestimmungen zu gewährleisten. Dabei werden neben den organisatorischen Maßnahmen (Aufbau- und Ablauforganisation) vor allem die IT-Systeme und deren Einsatz einer eingehenden Prüfung unterzogen. Dazu zählen vor allem die Transaktionsüberwachung und das laufende Monitoring des Gesamtkundenbestandes durch das geprüfte Institut. Im Rahmen der testfallweisen Einzelfallprüfung werden Transaktionen und Kundenbeziehungen im Hinblick auf sanktionsrelevante Sachverhalte evaluiert. Augenmerk wird dabei auch auf eine vollständige und aktuelle Dokumentation zum Kunden selbst, aber auch zum jeweiligen Geschäftsfall gelegt. Je nach Geschäftsmodell wird auch das Akkreditiv- und Garantiegeschäft, das Wechselstuben- und Edelmetallgeschäft und die Zusammenarbeit mit Zahlungsdienstleistern in die Vor-Ort Prüfung mit einbezogen.

**Informationsaustausch:**

Ein Austausch über bewährte Verfahren sowie die Überarbeitung und Umsetzung von gemeinsamen Leitlinien, um die wirksame und einheitliche Umsetzung der EU-Sanktionsvorschriften zu gewährleisten, erfolgt auf europäischer Ebene und hat sich in der Praxis als wichtige Auslegungshilfe sowohl für Institute als auch für beaufsichtigende Behörden erwiesen. Die in § 3 Abs. 4 FM-GwG vorgesehene Befugnis zum Informationsaustausch mit der FMA ist als wichtiges Beispiel zur Stärkung der Zusammenarbeit relevanter nationaler Behörden zu nennen.

**Gesamtrisiko**

**Insbesondere in Anbetracht der Möglichkeiten, sanktionierte Personen, Organisationen oder Einrichtungen zu erkennen, Gelder einzufrieren und sanktionswidrige Transaktionen hintanzuhalten kann das Risiko von Sanktionsverletzungen maßgeblich reduziert werden. Zudem wird dem Finanzsektor von der FATF generell ein gutes Verständnis zu den Gefahren und Risiken in den relevanten Compliance-Bereichen zuerkannt. Ungeachtet dessen besteht aber für Institute ein inhärentes Risiko, für die Umgehung von sanktionsrechtlichen Bestimmungen gegen Terrorismusfinanzierung missbraucht zu werden. Das Risiko daraus wird insgesamt als niedrig bis mittel eingestuft.**

**Empfehlungen**

In Anbetracht der Darlegungen zu möglichen Herausforderungen iZm grenzüberschreitenden Transaktionen, erscheint die Forcierung des (grenzüberschreitenden) Austausches zwischen Behörden zweckmäßig.

# Sektorrisikoanalyse Rechtsanwälte

## Sektor der Rechtsanwaltschaft

### Allgemeine Informationen

#### 1.1. Anzahl der Berufsträger

In Österreich gab es per Stichtag 31.12.2020 **6.605 Rechtsanwälte** und **2.270 Rechtsanwaltsanwärter**.

#### 1.2. Tätigkeitsbereiche (Verhältnis Geschäftsfeldverteilung)

Der Rechtsanwalt als Berater, Beistand oder Vertreter seiner Klienten in allen ihren öffentlichen und privaten Angelegenheiten wird in folgenden Bereichen tätig:

- Vertretung vor Zivilgerichten / Schiedsgerichten und Beratung in Bezug auf die Einleitung oder Vermeidung zivilrechtlicher Verfahren (27,6%),
- Vertretung vor Strafgerichten und in strafrechtlichen Ermittlungsverfahren (6,5%),
- Vertretung vor Verwaltungsbehörden und Beratung in Bezug auf Verwaltungsverfahren (9,8%),
- Vertretung und Beratung in familienrechtlichen Angelegenheiten (8,5%),
- Vertretung und Beratung in erbrechtlichen Angelegenheiten und Fragen der Vermögensnachfolge (6,1%),
- Mitwirkung bei der Planung und Durchführung bei Kauf oder Verkauf von Immobilien oder Unternehmen (19,5%),
- Mitwirkung bei der Planung und Durchführung bei der Verwaltung von Geld, Wertpapieren oder sonstigen Vermögenswerten, der Eröffnung oder Verwaltung von Bank-, Spar- oder Wertpapierkonten (1,6%),
- Mitwirkung bei der Planung und Durchführung bei der Gründung, dem Betrieb oder der Verwaltung von Trusts, Gesellschaften, Stiftungen oder ähnlichen Strukturen, einschließlich der Beschaffung der zur Gründung, zum Betrieb oder zur Verwaltung von Gesellschaften erforderlichen Mittel (6,3%) sowie
- sonstige Tätigkeiten (14,1%, darunter fallen Erwachsenenvertretung, Insolvenzverwaltung, Forderungsbetreibung, Organisation der Kanzlei).

Nach der Auswertung einer unter den Mitgliedern erhobenen repräsentativen Umfrage, bei der u.a. die Anteile obiger Bereich an der jeweiligen rechtsanwaltlichen Tätigkeit abgefragt wurde, sind gerundet 27% der rechtsanwaltlichen Geschäftsfelder im Bereich der geldwäschegeneigten Geschäfte angesiedelt; bei 73% der Tätigkeiten besteht hingegen kein Zusammenhang zu geldwäschegeneigten Geschäften.

#### 1.3. Kanzleistruktur

Der Großteil der Rechtsanwälte arbeitet in sehr kleinen Strukturen. Alleine die Hälfte der Rechtsanwälte ist als Einzelrechtsanwalt tätig. Ein weiteres Viertel der Rechtsanwälte arbeitet in Kleinstrukturen bestehend aus bis zu drei Rechtsanwälten.

#### 1.4. Spezifika der Berufsgruppe der Rechtsanwälte

Rechtsanwälte haben besonders strenge Ausbildungs- und Zulassungserfordernisse. Grundvoraussetzungen für die Tätigkeit als Rechtsanwalt sind der Abschluss eines Studiums des



österreich. Rechts an einer Universität und eine fünfjährige praktische Berufsausbildung, davon mindestens sieben Monate bei Gericht oder einer Staatsanwaltschaft und mindestens drei Jahre in der Kanzlei eines Rechtsanwaltes. In dieser Zeit müssen vorgeschriebene Ausbildungsveranstaltungen verschiedenster Themenbereiche absolviert werden. Erst nach positiv abgelegter Rechtsanwaltsprüfung und einer positiven Beurteilung der Vertrauenswürdigkeit erfolgt die Erteilung der Berechtigung zur Berufsausübung durch Hoheitsakt.

Die besonders qualifizierte Ausbildung garantiert ein hohes Maß an Fachwissen und beruflicher Erfahrung und ist der Rechtsanwalt damit ausgezeichneter Berater, Beistand oder Vertreter seiner Klienten in allen ihren öffentlichen und privaten Angelegenheiten. Der Rechtsanwalt ist außerdem zur ständigen Fort- und Weiterbildung verpflichtet.

Den neun Rechtsanwaltskammern obliegen die Wahrung der Ehre, des Ansehens und der Unabhängigkeit des Rechtsanwaltsstandes sowie die Wahrung der Rechte und die Überwachung der Pflichten der Rechtsanwälte. Die Rechtsanwaltskammern sind daher berechtigt, dem Rechtsanwalt in standesrechtlichen Fragen Empfehlungen, Ratschläge oder Weisungen zur Sicherstellung der Ehre und des Ansehens des Rechtsanwaltsstandes, aber auch zur Sicherstellung der Einhaltung standesrechtlicher Pflichten zu erteilen.

Die Beurteilung von Standesvergehen steht ausschließlich dem Disziplinarrat der jeweiligen Rechtsanwaltskammer zu. Zweite Instanz in Disziplinarsachen ist der Oberste Gerichtshof.

Der Rechtsanwalt unterliegt bei seiner Tätigkeit der Aufsicht und Disziplinierung durch die jeweilige Rechtsanwaltskammer. Eine Berufspflichtenverletzung kann bis zur Untersagung der Ausübung der Rechtsanwaltschaft führen.

#### **1.5. Allgemeine berufsrechtliche Sorgfaltspflichten und deren Verstärkung im Bereich GW/TF**

Der Rechtsanwalt hat unter Bedachtnahme auf seine konkrete Geschäftstätigkeit sowie auf Art und Größe seiner Kanzlei und unter Berücksichtigung bestimmter Risikofaktoren eine individuelle Analyse und Bewertung des Risikos seiner rechtsanwaltlichen Tätigkeit vorzunehmen. Er hat dabei zu prüfen, ob und inwieweit, ausgehend von der Struktur seiner Kanzlei, seiner Klienten und der von ihm für seine Klienten angebotenen Leistungen, er bzw. seine Mitarbeiter zu Zwecken der Geldwäsche missbraucht werden können. Dabei sind die Risikoanalyse auf Unionsebene sowie die nationale Risikoanalyse zu beachten.

Die vorgenommene Bewertung und deren Ergebnisse sind schriftlich aufzuzeichnen und regelmäßig zu aktualisieren bzw. auf ihre Aktualität zu prüfen.

Basierend auf dieser kanzleiinternen Risikoanalyse hat der Rechtsanwalt angemessene und geeignete Strategien und Verfahren zur Erfüllung der ihm im Rahmen der Bekämpfung der Geldwäscherei und Terrorismusfinanzierung auferlegten Sorgfaltspflichten hinsichtlich der Parteien, Verdachtsmeldungen, der Aufbewahrung von Aufzeichnungen, interner Kontrolle, Risikobewertung und Risikomanagement sowie zur Sicherstellung der Einhaltung der einschlägigen Vorschriften und der Kommunikation innerhalb seiner Kanzlei einzuführen und aufrechtzuerhalten, um Transaktionen, die mit Geldwäscherei oder Terrorismusfinanzierung zusammenhängen, vorzubeugen und zu verhindern. Der Rechtsanwalt hat sich selbst, die Rechtsanwaltsanwärter sowie die sonstigen bei ihm Beschäftigten durch geeignete Maßnahmen mit den Bestimmungen, die der Verhinderung oder Bekämpfung der Geldwäscherei und Terrorismusfinanzierung dienen, vertraut zu machen.

Unabhängig davon, ob ein geldwäschegeeignetes Geschäft im Sinne des § 8a Abs. 1 RAO vorliegt, ist ein Rechtsanwalt auch bei jeder Treuhandabwicklung (Surrogat des Zug-um-Zug-Prinzips), die über ein Anderkonto erfolgt, verpflichtet, die Identität der Person auf deren Rechnung die Gelder erliegen, festzustellen (§ 9a RAO und § 43 RL-BA) und dem Kreditinstitut bekannt zu geben. Diese Verpflichtung besteht auch bei nicht-geldwäschegeeigneten Geschäften.

### 1.6. Verschwiegenheitspflicht (professional secrecy)

Rechtsanwälte sind unabhängige Vertreter und Berater, die nur ihren Klienten verpflichtet und verantwortlich sind. Sie schützen und verteidigen die Rechte des Einzelnen auch gegenüber dem Staat und setzen diese durch. Das besondere Vertrauensverhältnis der Rechtsanwälte zu ihren Mandanten liegt in der gesetzlich verankerten anwaltlichen Verschwiegenheit, die Grundlage der Unabhängigkeit und Freiheit von Interessenkollisionen ist.

Nach der Rechtsprechung des EGMR kommt dem Rechtsanwalt eine besondere Stellung zu. Ihm gebührt ein besonderer Schutz bei der Kommunikation mit seinem Mandanten. Jeder Eingriff muss durch Gesetz vorgesehen und in einer demokratischen Gesellschaft gerechtfertigt und verhältnismäßig sein. Das Berufsgeheimnis und die Verschwiegenheitspflicht der Rechtsanwälte sind aber unabdingbar im Lichte der Vorgaben der Artikel 8 und 6 EMRK: Der Schutz des Berufsgeheimnisses stellt eine notwendige Garantie für die effektive Gewährleistung des Rechts auf ein faires Verfahren dar.

Gemäß § 9 Abs. 4 RAO hat bei Vorliegen eines der im § 8a Abs. 1 RAO angeführten Geschäfte der Rechtsanwalt dem Bundesminister für Inneres (Bundeskriminalamt, Geldwäschemeldestelle gemäß § 4 Abs. 2 Bundeskriminalamt-Gesetz) auf Anfrage über alle ihm bekannten Umstände Auskunft zu erteilen, soweit dies zur Klärung eines gegen die Partei gerichteten Verdachts auf Geldwäscherei (§ 165 StGB) oder Terrorismusfinanzierung (§ 278d StGB) erforderlich ist.

Die Bestimmungen der §§ 8a ff. RAO regeln die von jedem Rechtsanwalt einzuhaltenden Sorgfaltsmaßnahmen, um so früh wie möglich zu verhindern, dass er und seine Kanzlei für Zwecke der Geldwäsche missbraucht werden. Wirkt ein Rechtsanwalt an einem Geschäft mit, bei dem die Gelder aus einer kriminellen Vortat im Sinne des § 165 StGB stammen, stellt das nicht nur einen Verstoß gegen berufsrechtliche Pflichten dar, sondern kann er sich dadurch selbst strafbar machen (Geldwäscherei (§ 165 StGB)); dasselbe gilt für eine Beteiligung an einer Terrorismusfinanzierung (§ 278d StGB).

Wie oben ausgeführt, ist darauf hinzuweisen, dass nicht die gesamte rechtsanwaltliche Tätigkeit GW/TF-relevant ist. Der überwiegende Teil der rechtsanwaltlichen Tätigkeit ist in der Tat nicht geldwäschegeneigt. Darunter fallen etwa die Vertretung vor Zivilgerichten / Schiedsgerichten und die Beratung in Bezug auf die Einleitung oder Vermeidung zivilgerichtlicher Verfahren, die Vertretung vor Strafgerichten und in strafrechtlichen Ermittlungsverfahren, die Vertretung vor Verwaltungsbehörden und Beratung in Bezug auf Verwaltungsverfahren, die Vertretung und Beratung in familienrechtlichen Angelegenheiten, die Vertretung und Beratung in erbrechtlichen Angelegenheiten sowie die Erstellung von Verträgen im Bereich nicht geldwäschegeneigter Geschäfte.

#### Sektor / Produkt / Dienstleistung / Aktivität

Nachfolgende Ausführungen betreffen in Orientierung an den Katalog der geldwäschegeneigten Geschäfte des § 8a RAO folgende GW/TF-geneigte Produkte/Dienstleistungen:

- Kauf oder Verkauf von Immobilien (einschließlich der Treuhandabwicklung)
- Kauf oder Verkauf von Unternehmen (einschließlich der Treuhandabwicklung)
- Verwaltung von Geld, Wertpapieren oder sonstigen Vermögenswerten
- Eröffnung oder Verwaltung von Bank-, Spar- oder Wertpapierkonten
- Gründung, Betrieb, Verwaltung von Trusts, Gesellschaften, Stiftungen oder ähnlichen Strukturen einschließlich Beschaffung der zur Gründung, zum Betrieb oder zur Verwaltung von Gesellschaften erforderlichen Mittel

Eine detaillierte Analyse für die einzelnen GW/TF-geneigten Produkte/Dienstleistungen erfolgt im Rahmen der Sektorrisikoanalyse.

## Generelle Beschreibung

Beim Kauf oder Verkauf von Immobilien umfasst die Tätigkeit der Rechtsanwälte u.a. die Vertragsverhandlungen mit den Parteien, die Errichtung des Kaufvertrages, die treuhändige (Zug-um-Zug) Abwicklung des Austauschs der wechselseitig zu erbringenden Leistungen, die Selbstberechnung der Steuern, die Einholung allenfalls erforderlicher Genehmigungen (Grundverkehr, Forstwirtschaft, Liegenschaftsteilung, Raumplanung usw.) die grundbücherliche Durchführung.

Beim Kauf oder Verkauf von Unternehmen umfasst die Tätigkeit der Rechtsanwälte u.a. die Vertragsverhandlungen mit den Parteien, die Errichtung der Verträge, die Errichtung des Gesellschaftsvertrages, gegebenenfalls die treuhändige (Zug-um-Zug) Abwicklung der Kaufpreiszahlung und der Anteils- bzw. Vermögensübertragung samt den weiteren Durchführungshandlungen, insbesondere der Einholung allenfalls erforderlicher Genehmigungen (Grundverkehr; kartellgerichtliche Genehmigung; Genehmigung nach dem AußWG, etc.), die Selbstberechnung der Steuern und die Durchführung im Firmenbuch.

Die Verwaltung von Geld, Wertpapieren oder sonstigen Vermögenswerten erfolgt regelmäßig in der Funktion als (gerichtlich bestellter) Erwachsenenvertreter und Insolvenzverwalter. Davon abgesehen verwaltet der Rechtsanwalt Geldwerte fast ausschließlich im Rahmen von Abwicklungs-Treuhandschaften im Zusammenhang mit dem Kauf und Verkauf von Immobilien oder Unternehmen.

Die Eröffnung oder Verwaltung von Bank-, Spar- oder Wertpapierkonten erfolgt in aller Regel im Zusammenhang mit der Ausführung von Abwicklungstreuhandschaften im Zusammenhang mit dem Verkauf von Liegenschaften und Unternehmensanteilen, allenfalls im Rahmen von Organfunktionen.

Rechtsanwälte wirken im Rahmen ihrer Tätigkeit an der Gründung und Betrieb von Gesellschaften und Privatstiftungen mit. Weiters wirken Rechtsanwälte als Mitglied der Organe von Privatstiftungen (Vorstand, Beirat) an der Geschäftsführung sowie Verwaltung des Stiftungsvermögens, einschließlich der Auszahlung von Begünstigungen an Begünstigte mit; Rechtsanwälte nehmen auch Aufsichtsratsfunktionen in Gesellschaften wahr und überwachen dabei die Geschäftsführung durch den Vorstand.

## Bedrohung

### **Terrorismusfinanzierung:**

In der SNRA wurde die Bedrohung, dass Dienstleistungen der Rechtsanwälte für terroristische Aktivitäten missbraucht werden, mit einem sehr hohen Risiko eingestuft und ausgeführt, dass die Bewertung der TF-Bedrohung im Zusammenhang mit Rechtsdienstleistungen von Rechtsanwälten in Verbindung mit dem Punkt GW betrachtet wird; dieser Systematik folgend zeigt sich bei der Österreich-spezifischen Bedrohungslage zu beiden Punkten, dass nicht nur die Ausgestaltung des Berufs des Rechtsanwalts in Österreich und das zur Anwendung kommende Aufsichtsregime, sondern generell eine gerade in letzter Zeit noch einmal gesteigerte Aufmerksamkeit im Bereich der Terrorismusbekämpfung dazu führt, dass die länderspezifische Bedrohungssituation in Österreich gegenüber der in der SRNA vorgenommenen Einordnung abgemildert erscheint.

### **Conclusio:**

**Die Bedrohung im Bereich Terrorismusfinanzierung ist als mittel einzustufen.**

**Geldwäscherei:**

Rechtsanwälte haben eine besondere Vertrauensstellung in der Gesellschaft. Durch die Beziehung eines Rechtsanwalts bzw. die Abwicklung des Geschäfts über diesen sollen mitunter Unbedenklichkeit, Bonität, Legitimität und Seriosität signalisiert werden.

Kriminelle könnten versuchen, komplexe bzw. undurchsichtige Strukturen zu schaffen, an denen viele Jurisdiktionen beteiligt sind, insbesondere Offshore-Rechtsordnungen mit geheimen Eigentumsketten, bei denen der Eigentümer eines anderen Unternehmens oder einer anderen Rechtsstruktur an anderer Stelle registriert ist. Durch diese Kombination aus Rechtsdienstleistungen kann versucht werden der Transaktion Komplexität hinzuzufügen.

Ein erhöhtes Bedrohungspotenzial betreffend Geldwäsche besteht beim Erwerb von Immobilien bzw. Unternehmen und Unternehmensanteilen durch Personen mit (Wohn-)Sitz außerhalb der EU/des EWR. An gelegentlich als Erwerber auftretende, oft nur für Zwecke des konkreten Erwerbs errichtete (meist inländische) Erwerbsgesellschaften sind gegebenenfalls über viele Stufen und kompliziert verschachtelt Rechtsträger beteiligt, bei denen sich die Feststellung der wirtschaftlichen Eigentümer bzw. auch die Herkunft der Mittel in Österreich selbst unter Umständen sehr schwierig gestaltet. Vergleichbares gilt für Fälle der Errichtung von (Erwerbs-)Gesellschaften zum Zweck der Verwaltung von Vermögenswerten (wie beispielsweise Beteiligungen).

Das Bedrohungsszenario im Zusammenhang mit der Eröffnung und Verwaltung von Bank-, Spar- und Wertpapierkonten bzw. von Trusts, Stiftungen und ähnlichen Strukturen durch Rechtsanwälte erscheint insgesamt weniger ausgeprägt, zumal gerade bei Übernahme solcher Aufgaben durch in Österreich tätige Rechtsanwälte die Sensibilität inzwischen wesentlich erhöht ist, als dies etwa im internationalen Transaktionsgeschäft der Fall wäre.

**Conclusio:**

**Ebenso wie bei der Terrorismusfinanzierung führen die berufsrechtlichen und allgemeinen Rahmenbedingungen dazu, dass die Bedrohung als mittel einzustufen ist.**

**Verletzbarkeit****Terrorismusfinanzierung:**

Die Bewertung der Verletzbarkeit durch Terrorismusfinanzierung im Zusammenhang mit Rechtsdienstleistungen von Rechtsanwälten wird grundsätzlich in Verbindung mit Geldwäscherei-Modellen betrachtet, die dazu dienen sollen die illegale Herkunft der Gelder zu verbergen.

Hinzuweisen ist aber, dass nur eine geringe Wahrscheinlichkeit besteht, dass der Kauf oder Verkauf von Immobilien zur Terrorismusfinanzierung missbraucht wird. Es müssten jedenfalls zusätzliche Elemente, wie die Weiterleitung des Verkaufserlöses an dubiose Vereine, entsprechende Staaten oder an entsprechende Personen hinzutreten. In diese ist der Rechtsanwalt in der Regel aber gerade nicht eingebunden.

Die Involvierung eines Rechtsanwalts in Kauf und Verkauf von Unternehmen zu Terrorismusfinanzierung ist auch eher atypisch, da Terrorismusfinanzierung in der Regel rasch flüssige Mittel benötigt und sich daher nachhaltige Investitionen in Unternehmen für Zwecke der Terrorismusfinanzierung nicht eignen. Bei Unternehmenstransaktionen müssten daher weitere Umstände, insbesondere hinsichtlich der Weiterleitung eines Verkaufserlöses an entsprechende Empfänger hinzukommen, in die Rechtsanwälte aber gerade nicht involviert werden bzw. die auch nicht mehr zur (typischen) Unternehmenstransaktion gehören.

**Conclusio:**

**Ausgehend von der SNRA, die eine hohe Verletzbarkeit nahelegt, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von Rechtsanwälten für die Zwecke der Terrorismusfinanzierung missbraucht zu werden, mit gering einzustufen ist.**

**Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von Rechtsanwälten im Hinblick auf den Missbrauch für die Zwecke der Geldwäscherei als hoch eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden:

**(a) Risikopotential:**

Da Rechtsanwälte häufig in kleinen Struktureinheiten organisiert und tätig sind, könnten Täter eine Chance auf fehlende Sensibilität und Wachsamkeit bei GW-Risiken sehen. Auch kann es sein, dass Rechtsanwälte in die Verwaltung komplexer rechtlicher Situationen eingebunden sind und das Verhalten der Kunden noch eher unbekannte „red flags“ auslöst.

**(b) Risikobewusstsein:**

Die Rechtsanwaltskammern sind zur Überprüfung der Einhaltung der Bestimmungen nach § 8a ff RAO durch ihre Mitglieder verpflichtet und ergreifen vielfältige Schritte bei der Überwachung der GW/TF-Verpflichtungen ihrer Mitglieder. Die Rechtsanwaltskammern prüfen bei Vor-Ort-Prüfungen, ob Rechtsanwälte, Rechtsanwaltsanwärter und Kanzleipersonal die gesetzlichen Bestimmungen bezüglich Verhinderung von GW/TF einhalten. Im Rahmen der Klientengelder- bzw. Treuhandprüfung wird auch die Einhaltung sonstiger gesetzlicher Bestimmungen (z. B. hinsichtlich des wirtschaftlichen Eigentums) überprüft. Es wird u.a. geprüft, ob eine schriftliche Kanzlei-Risikoanalyse vorliegt und welche Strategien zur Verhinderung von GW/TF abgeleitet werden (z.B. Kanzleileitfäden, Mitarbeiterschulungen, Bestimmung eines Geldwäschebeauftragten etc.). Durchschnittlich wurden in den letzten vier Jahren ca. 20 % aller Rechtsanwälte jährlich überprüft.

Im Zuge der Vor-Ort-Prüfungen wird u.a. geprüft, ob bei geldwäschegeneigten Geschäften die Identität der Parteien und, der wirtschaftliche Eigentümer festgestellt und dokumentiert wurde, ob es Verdachtsmeldungen gab und ob die entsprechende Dokumentation vorliegt. Diese Überprüfungen werden sowohl stichprobenartig als auch anlassbezogen bei Vorhandensein von Verdachtsmomenten durchgeführt. Die Prüfungsergebnisse zeigen, dass die gesetzlichen Vorgaben weitestgehend beachtet und insbesondere die Feststellung der wirtschaftlichen Eigentümer praktisch lückenlos durchgeführt wird.

Aufgrund dessen kann festgehalten werden, dass ein hohes Risikobewusstsein in der Rechtsanwaltschaft besteht.

**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Der Umstand, dass neben dem Rechtsanwalt regelmäßig auch weitere Verpflichtete und Behörden in das Zustandekommen und die Abwicklung eines Geschäfts involviert sind, führt in aller Regel zu keiner Vernachlässigung der die Rechtsanwälte zur Verhinderung von Geldwäscherei und Terrorismusfinanzierung treffenden Pflichten, sondern hat vielmehr zur Folge, dass diesen Pflichten besonderes Augenmerk geschenkt wird. Dies deshalb, weil eine Nachlässigkeit bei der Erfüllung der eigenen Verpflichtungen nicht zuletzt das erhebliche Risiko in sich birgt, dass dies bei der eigenständigen Wahrnehmung der Verpflichtungen durch eine andere in das System der Bekämpfung von Geldwäscherei und Terrorismusfinanzierung involvierte Person/Einrichtung (wie etwa ein Kreditinstitut) hervorkommt und als Folge daraus erhebliche Nachteile für den seine Pflichten vernachlässigenden Rechtsanwalt

drohen. Entsprechendes gilt auch für die durch die Rechtsanwaltskammer ausgeübte Aufsicht, angesichts derer jedem Rechtsanwalt bewusst ist, dass mit Geldwäscheprüfungen jedenfalls zu rechnen ist. Auch dies erhöht die Sensibilität in diesem Bereich ganz wesentlich.

So ist bei Immobilientransaktionen eine Eintragung im gerichtlich geführten Grundbuch erforderlich. Zu erfolgen hat überdies die Berechnung und Abführung der Immobilienertragsteuer, Grunderwerbsteuer, Eintragungsgebühr samt entsprechender Meldungen an die Finanzbehörden. Diese Selbstberechnung durch die Parteienvertreter liegt insbesondere auch im Interesse der Finanzverwaltung, die dadurch eine erhebliche Entlastung erfährt. Durch die Finanzverwaltung erfolgt dann wiederum im Wege von besonderen Betriebsprüfungen (Außenprüfungen) eine Überprüfung, ob die Selbstberechnung korrekt erfolgt ist.

Bei Immobilientransaktionen mit Käufern aus Drittstaaten (Ausländergrunderwerb) erfolgt außerdem eine Prüfung des wirtschaftlichen Eigentümers durch die Behörden. Besonders bedeutsam ist, dass der Zahlungsfluss, soweit er – wie im Regelfall – über Bankkonten erfolgt, auch und besonders auf Ebene der Banken überprüft wird; zudem läuft die Abwicklung der Geldtransaktionen über die Treuhandinrichtungen der Rechtsanwaltskammern, die im Rahmen ihrer Aufsicht zur Einsicht berechtigt sind.

Schließlich bedarf eine Immobilientransaktion der notariellen Beglaubigung, bei der eine zusätzliche Identitätsprüfung der handelnden Personen durch den Notar erfolgt.

Die rechtlichen Rahmenbedingungen entsprechen dem aktuellen Stand der EU-Geldwäscherichtlinien. Durch die Einhaltung organisatorischer Maßnahmen (insbesondere Risikoanalysen, Schulungen und strukturierte Prozesse) in der Kanzlei wird sichergestellt, dass im Zuge der Aufnahme neuer Klienten, der Annahme von Mandaten und der Betreuung laufender Geschäftsbeziehungen die GW/TF-Risiken adäquat berücksichtigt werden.

Die Aufsicht über die Rechtsanwaltschaft im Bereich GW/TF erfolgt durch die neun Rechtsanwaltskammern, die regelmäßige sowie ad-hoc-Kontrollen durchführen. Die Aufsicht umfasst dabei nicht nur die Überprüfung einzelner Mandate, sondern auch die Einhaltung organisatorischer Maßnahmen in der Kanzlei. Verletzungen können weitreichende disziplinarische Sanktionen nach sich ziehen.

#### **Human- und Finanzressourcen:**

In den neun Rechtsanwaltskammern hatten 2020 gesamt 146 Personen mit der Aufsicht im Zusammenhang mit der Prävention von GW/TF zu tun.

#### **Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die an sich eine hohe Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von Rechtsanwälten für die Zwecke der Geldwäscherei missbraucht zu werden, in Österreich mit mittel einzustufen ist.**

#### **Risikomindernde Maßnahmen**

Neben den bereits oben genannten risikomindernden Maßnahmen sind weiters folgende Maßnahmen zu nennen, die das Risiko auch pro futuro weiter mindern:

- Verstärkte Einzelfallanalysen und risikobasierter Prüfungsansatz der Kammern: Zu berücksichtigen ist, dass die Aus- und Bewertungen der Risikoanalysen der einzelnen Berufsträger verstärkt sowohl inhaltlich wie auch organisatorisch in die Aufsicht einfließen,

- auch im Bereich der Fortbildung sollen die Erkenntnisse aus der Aufsichtstätigkeit gezielt berücksichtigt werden,
- strenge disziplinarrechtliche Konsequenzen bei Verstößen gegen die berufsrechtlichen Vorschriften,
- kanzleibezogene Risikoanalyse und mandatspezifische Überprüfung,
- verstärkte Vernetzung und Zusammenarbeit mit anderen Stellen und Verpflichteten: Zu nennen sind hier allen voran die FIU (Geldwäsche-Meldestelle) sowie das bereits geschaffene Register der wirtschaftlichen Eigentümer. Rechtsanwälte sind gemäß § 9 WiEReG zur Einsicht berechtigt. Insbesondere die Erkenntnisse aus der Vernetzung mit der FIU fließen dabei wieder unmittelbar in die Informationen an die Rechtsanwälte bzw. Schulungen ein,
- zudem ist auf die mit der Abwicklungstreuhanderschaft verbundenen Sicherungsinstrumente (Treuhandregister, Abwicklung über anerkanntes Kreditinstitut) zu verweisen.

#### **Gesamtrisiko**

**Das Gesamtrisiko ist als mittel einzustufen.**

#### **Empfehlungen**

- Weiterführung der Schulungen und Fortbildungsmaßnahmen,
- vermehrte Durchführungen von Off-Site-Überprüfungen durch Rechtsanwaltskammern,
- mehr aktuelle Informationen der FIU über Methoden der Geldwäscherei und der Terrorismusfinanzierung und über Anhaltspunkte, aus denen sich verdächtige Transaktionen erkennen lassen

# Sektorrisikoanalyse Notariat

<b>Notare</b>
<b>Allgemeine Informationen</b>
<p><b>1.1. Allgemeines</b></p> <p>In Österreich gibt es (mit Stand 31.10.2020) 522 Notarstellen, mit 519 Notaren und 582 Notariatskandidaten. Rund 76 % der Amtsstellen werden als Einzelnotariate geführt, rund 24 % als Partnerschaften. Der Tätigkeitsbereich des Notars reicht von der juristischen Beratung über die Erkundung des Willens der Parteien und der Beglaubigung von Dokumenten bis zur Ausübung von Tätigkeiten für den Staat. Die österreichischen Notare sind prinzipiell Generalisten. Das bedeutet einerseits, dass jeder Notar die gleichen Rechtsdienstleistungen erbringen kann und deshalb alle von den im Folgenden beschriebenen Tätigkeitsfelder abdeckt, und andererseits, dass der Notar seine Befugnisse an sich im gesamten Bundesgebiet ausüben darf. Der gesetzlich bestimmte Wirkungsbereich der Notare umfasst folgende Tätigkeiten:</p> <p><b>Errichtung öffentlicher Urkunden; Verfassung von Privaturkunden/Parteienvertretung; Treuhandabwicklung; Mediator; Gerichtskommissariat.</b></p>
<p><b>1.2. Geschäftsfeldverteilung</b></p> <p>Die Notare üben die im gesetzlich bestimmten Wirkungsbereich festgelegten Tätigkeiten in verschiedenen Geschäftsfeldern aus. Die notarielle Geschäftsfeldverteilung nach Umsätzen (in %) stellen sich wie folgt dar:</p> <ol style="list-style-type: none"><li>Mitwirkung an der Planung oder Durchführung von <b>Kauf oder Verkauf von Immobilien</b>, inkl. Abwicklungstreuhandchaft: 28,8 %</li><li>Mitwirkung an der Planung oder Durchführung von <b>Kauf oder Verkauf von Unternehmen</b>, inkl. Abwicklungstreuhandchaft: 6,6 %</li><li>Mitwirkung an der Planung oder Durchführung der <b>Verwaltung von Geld, Wertpapieren oder sonstigen Vermögenswerten</b>, der Eröffnung oder Verwaltung von Bank-, Spar- oder Wertpapierkonten im Rahmen von <b>Kuratortätigkeiten</b>): 0,8 %</li><li>Mitwirkung an der Planung oder Durchführung der <b>Verwaltung von Geld, Wertpapieren oder sonstigen Vermögenswerten</b>, der Eröffnung oder Verwaltung von Bank-, Spar- oder Wertpapierkonten als <b>Vorsorgebevollmächtigter oder Erwachsenenvertreter</b>: 0,7 %</li><li>Mitwirkung an der Planung und Durchführung der <b>Verwaltung von Geld, Wertpapieren oder sonstigen Vermögenswerten</b>, der Eröffnung oder Verwaltung von Bank-, Spar- oder Wertpapierkonten in <b>sonstigen Fällen</b>: 0,6 %</li><li>Mitwirkung an der Planung oder Durchführung der <b>Gründung von Gesellschaften oder Stiftungen</b> einschließlich der Beschaffung der zur Gründung, zum Betrieb oder zur Verwaltung von Gesellschaften erforderlichen Mittel und damit verbundenen Treuhandchaften: 8,7 %</li><li>Mitwirkung am <b>Betrieb oder der Verwaltung von Gesellschaften oder Stiftungen</b> einschließlich der Beschaffung der zum Betrieb oder zur Verwaltung von Gesellschaften erforderlichen Mittel, zB. im Rahmen von Vorstandsmandaten: 0,8 %</li><li>Mitwirkung an der Planung oder Durchführung der <b>Gründung, des Betriebs oder der Verwaltung von Trusts oder ähnlichen Strukturen</b>, einschließlich der Beschaffung der zur Gründung, zum Betrieb oder zur Verwaltung erforderlichen Mittel: 0,2 %</li></ol>



- i. **Gerichtskommissärstätigkeit in Verlassenschaften:** 21 %
- j. **Gerichtskommissärstätigkeit** durch Einsicht in **Firmenbuch und Grundbuch:** 3,9 %
- k. Vertretung und Beratung in **familienrechtlichen Angelegenheiten** (zB. Adoption, Fortpflanzungsmedizinengesetz, Eheverträge): 4,4 %
- l. Vertretung und Beratung in **erbrechtlichen Angelegenheiten:** 11 %
- m. Tätigkeiten im Bereich der **Personenvorsorge:** 7,5 %
- n. Vertretung vor **Zivilgerichten / Schiedsgerichten / Strafgerichten** und Beratung in Bezug auf die Einleitung oder Vermeidung von Verfahren: 0,3 %
- o. Vertretung vor (**Verwaltungs**)**Behörden** und Beratung in Bezug auf Verwaltungsverfahren: 1,4 %
- p. Tätigkeit als **Mediator:** 0,1 %
- q. **Sonstige Tätigkeiten:** 3,3 %

47,2% der notariellen Geschäftsfelder sind im Bereich der „geldwäschegeneigten Geschäfte“ im Sinn des § 36a NO (siehe oben Punkt 1.2. a. bis h.) angesiedelt, bei 52,9% der notariellen Geschäftsfelder besteht kein Zusammenhang zu geldwäschegeneigten Geschäften (siehe oben Punkt 1.2. i. bis q.).

Eine Auswertung der Wohnsitze der Parteien der Notare (Treugeber) für das Jahr 2019 zeigt, dass die Parteien weitaus überwiegend aus Österreich (95,96 %) bzw. dem EU/EWR-Raum und der Schweiz (3,85 %) kamen. Parteien aus „sonstigen Ländern“ (welche hier noch nicht genannt wurden) machen einen Anteil von 0,19 % aus. Diese Parteien kommen insbesondere aus USA, Kanada, Australien, Liechtenstein und Bosnien und Herzegowina.

Lediglich 0,001 % der Parteien kamen im Jahr 2019 aus den Ländern der Delegierten Verordnung (EU) 2016/1675 der Europäischen Kommission (Afghanistan, Äthiopien, Bosnien und Herzegowina, Guyana, Irak, Jemen, Laos, Pakistan, Sri Lanka, Syrien, Tunesien, Trinidad und Tobago, Uganda, Vanuatu).

26,2 % der Notare haben Parteien, die als PEPs zu qualifizieren sind. Diese Parteien sind zu 96,3 % inländische PEPs, zu 3,7 % ausländisch PEPs.

Bei Anknüpfung der Geschäftsbeziehung oder der Durchführung des Geschäfts sind 95,6 % der Parteien physisch anwesend, bei 4,4 % handelt es sich um Ferngeschäfte (Parteien sind nicht anwesend).

### 1.3. Spezifika der Berufsgruppe der Notare

Der österreichische Notar ist freiberuflich tätiger Jurist, der seine Klienten berät und Verträge sowie öffentliche Urkunden errichtet. Er ist überwiegend im außerstreitigen und rechtsvorsorgenden Bereich tätig und führt den Amtstitel „öffentlicher Notar“. Seine Tätigkeit ist vor allem durch seine Unabhängigkeit und zum Teil hoheitliche Funktion gekennzeichnet (z.B. als Gerichtskommissär bei der Erfüllung inhaltlich richterlicher Aufgaben und bei der Errichtung öffentlicher Urkunden). In Abgrenzung zum Rechtsanwalt trifft den Notar (als Träger eines öffentlichen Amtes) eine Belehrungspflicht gegenüber allen Parteien und er hat die Interessen aller an einem Rechtsgeschäft Beteiligten gleichermaßen zu wahren. Jede Mitwirkung an verbotenen, verdächtigen oder zum Schein vorgegebenen Geschäften ist verboten (§§ 5 Abs. 3, 34 NO).

Der Notar unterliegt bei Erbringung seiner Dienstleistungen (Produkte) strengen berufsrechtlichen und disziplinarischen Regelungen und hat einen hohen Sorgfaltsmaßstab bei Erbringung seiner Dienstleistungen entsprechend den in der Notariatsordnung und in Richtlinien der Österreichischen Notariatskammer (nachfolgend ÖNK) zu gewährleisten.

Die oberste Aufsicht über das Notariatswesen ist dem Bundesminister für Justiz übertragen, die generelle Überwachung der Amtsführung der Notare den Präsidenten der Gerichtshöfe erster und zweiter Instanz. Die allgemeine und unmittelbare Berufsaufsicht über die Notare

in ihrem amtlichen Wirken, aber auch in ihrem standesgemäßen Verhalten obliegt der zuständigen Notariatskammer (nachfolgend NK, § 153 NO). Siehe dazu näher unter Punkt 2.2.2.

Die Neuschaffung, Auflassung und Verlegung von Notarstellen ist nur mittels Verordnung des Bundesministers für Justiz möglich („Systemisierung“).

## Methodologie

### 2.1 Produkte - GW/TF relevante Dienstleistungen

Nach § 36a NO ist der Notar *„im Hinblick auf die hier besonders hohe Gefahr der Geldwäscherei (§ 165 StGB) oder Terrorismusfinanzierung (§ 278d StGB) verpflichtet, alle Geschäfte besonders sorgfältig zu prüfen, bei denen er im Namen und auf Rechnung seiner Partei Finanz- oder Immobilientransaktionen durchführt oder für seine Partei an deren Planung oder Durchführung mitwirkt und die Folgendes betreffen:*

1. *den Kauf oder den Verkauf von Immobilien oder Unternehmen,*
2. *die Verwaltung von Geld, Wertpapieren oder sonstigen Vermögenswerten, die Eröffnung oder Verwaltung von Bank-, Spar- oder Wertpapierkonten oder*
3. *die Gründung, den Betrieb oder die Verwaltung von Trusts, Gesellschaften, Stiftungen oder ähnlichen Strukturen, einschließlich der Beschaffung der zur Gründung, zum Betrieb oder zur Verwaltung von Gesellschaften erforderlichen Mittel.“*

Diese weite Definition der „geldwäschegeneigten“ Geschäfte umfasst große Teile der notariellen Tätigkeit, vor allem im Bereich der Finanz- und Immobilientransaktionen. Insgesamt beträgt der Anteil der Tätigkeiten in Bezug auf „geldwäschegeneigte Geschäfte“ innerhalb der Berufsgruppe der Notare 47,2 % (siehe dazu näher Punkt 1.2. a. bis h.).

Die restlichen 52,8 % (siehe näher oben Punkt 1.2. i. bis q.) der notariellen Dienstleistungen zählen entweder nicht zu den „geldwäschegeneigten Geschäften“ oder sie betreffen zwar per definitionem „geldwäschegeneigte Geschäfte“, sind aber dennoch aus verschiedenen Gründen nicht bzw. kaum GW/TF gefährdet.

#### 2.2.1. Die „Abwicklungstreuhandschaft“

Die Mehrzahl der geldwäschegeneigten Geschäfte, bei denen der Notar in einen Zahlungsvorgang eingebunden ist, wird mittels notarieller Treuhandschaft (zwecks Sicherung einer Zug-um-Zug Abwicklung durch den Notar zur Wahrung der Interessen von Käufer und Verkäufer) abgewickelt, die ab einem Treuhandrahmen von € 10.000,- in das Treuhandregister (THR) der ÖNK eingetragen werden müssen. Das Produkt Treuhandschaften ist in der Praxis so gut wie immer mit den geldwäschegeneigten Immobilien- und Gesellschaftsrechtstransaktionen verbunden.

Anzahl der Registrierungen im THR: 2017 43.435; 2018 44.591; 2019: 48.156.

Die durchschnittliche Höhe (Gesamtrahmen) einer Treuhandschaft betrug: 2017 EUR 259.526,-; 2018 EUR 278.625,-; 2019 EUR 295.716,-.

Dabei war durchschnittlich folgende Anzahl von Treugebern an einer Treuhandschaft beteiligt: 2017 2,97; 2018 2,99; 2019 3,02.

Bei der **Notartreuhandbank AG (NTB)** als derzeit einzigem zur Abwicklung notarieller Treuhandschaften befugten und anerkannten Kreditinstitut wurden folgende Treuhandkonten durch Notare eröffnet: 2017: 41.594; 2018: 42.556; 2019: 53.268, die im Jahr 2019 durchschnittlich für die Dauer von 4 Monaten und 21 Tagen eröffnet waren. Die NTB führt ausschließlich auf den Namen der Notare lautende Anderkonten, die strengsten, durch Gesetz und Richtlinien (insbesondere THR 1999) festgelegten Transparenz- und Sicherheitsanforderungen entsprechen müssen. Notare dürfen keine Konten für eigene Geschäfte bei der NTB eröffnen.

### **2.2.2. Revisionen, Schulungs- und Informationsmaßnahmen**

Die NK sind verpflichtet, regelmäßig die Akten, Geschäftsregister, Bücher, Verzeichnisse, Sammlungen und den Geschäftsbetrieb der Notare insgesamt zu überprüfen (§ 154 Abs. 1 NO, „Revision“). Dabei ist insbesondere zu überwachen, ob die Notare die Bestimmungen einhalten, die der Verhinderung oder der Bekämpfung der Geldwäscherei oder der Terrorismusfinanzierung (nachfolgend GW/TF) dienen. In Verdachtsfällen werden auch unangekündigte Zwischen- bzw. Sonderprüfungen von der NK durchgeführt (außerordentliche Revision). Fällt der NK im Rahmen der Revision oder bei anderer Gelegenheit ein Mangel oder Verstoß auf, hat sie - je nach Schwere - eine angemessene Erinnerung zu erteilen, ein Ordnungsstrafverfahren durchzuführen oder ein Disziplinarverfahren durch das Oberlandesgericht als Disziplinargericht zu veranlassen. Stößt die NK auf Tatsachen, die mit GW/TF zusammenhängen, so hat sie außerdem eine Verdachtsmeldung an die Geldwäsche-Meldestelle zu erstatten (§ 36c Abs. 1 NO). Im Durchschnitt wird jede Notariatskanzlei ca. alle 3 bis 5 Jahre mindestens einmal überprüft (im Jahr 2017 gab es österreichweit 77 Kanzleirevisionen, 2018 gab es österreichweit 245 Kanzleirevisionen und 2019 waren es österreichweit 86 Kanzleirevisionen.).

Die ÖNK bietet zahlreiche, stark nachgefragte Seminare rund um das Thema Verhinderung und Bekämpfung von GW/TF an: im Jahr 2017 fanden 5 Seminare, im Jahr 2018 10 Seminare und im Jahr 2019 10 Seminare statt. Die ÖNK, stellt überdies den Landesmitgliedern seit 2008 einen laufend aktualisierten Leitfaden zum Thema GW/TF („Empfehlung der ÖNK zur Verhinderung von GW/TF“) elektronisch zur Verfügung und informiert die Landesmitglieder regelmäßig und anlassbezogen durch Rundschreiben und Aussendungen über wichtige Neuerungen in diesem Bereich.

48,2 % der Notariatskanzleien führen mehrmals pro Jahr, 43,6 % der Notariatskanzleien zumindest einmal pro Jahr und 6,2 % seltener als einmal pro Jahr kanzleiinterne Schulungen / Instruktionen zu diesen Themen durch. Dabei werden rund 60 % der Notare, rund 80 % der Notariatskandidaten, rund 26 % der sonstigen juristischen Mitarbeiter und rund 92 % der nicht-juristischen Mitarbeiter geschult. Zusätzlich erfolgen bei rund 68 % der Notariatskanzleien kanzleixterne Schulungen zum Thema Verhinderung von GW/TF, bei denen rund 91 % der Notare, rund 86 % der Notariatskandidaten, rund 8 % der sonstigen juristischen Mitarbeiter und rund 21 % der nicht-juristischen Mitarbeiter geschult werden.

#### **Produktspezifische Risikoanalyse**

Non-Financial Products, Punkt 10 „Legal services from notaries and other independent legal professions“ der SNRA SWD(2019) 650 (Seite 182ff, nachfolgend kurz „legal services“).

#### **Generelle Beschreibung**

Entsprechend Art. 2 Abs. 1 Z 3 lit b der Richtlinie (EU) 2018/843 und der SNRA (Seite 186) umfassen notarielle Dienstleistungen in Österreich folgende Bereiche (geldwäschegeneigte Geschäfte gemäß § 36a NO): Kauf/Verkauf von Immobilien, Kauf/Verkauf von Unternehmen, Verwaltung von Geld, Wertpapieren oder sonstigen Vermögenswerte, Eröffnung oder Verwaltung von Bank-, Spar- oder Wertpapierkonten und Gründung, Betrieb, Verwaltung von Trusts, Gesellschaften, Stiftungen oder ähnlichen Strukturen einschließlich Beschaffung der zur Gründung, zum Betrieb oder zur Verwaltung von Gesellschaften erforderlichen Mittel. In Orientierung an der SNRA SWD (2019) 650 sind diese Dienstleistungen unter Non-Financial Products, Punkt 10 „Legal services from notaries and other independent legal professions“ (nachfolgend kurz „legal services“) der SNRA SWD (2019) 650 (Seite 182ff) zu subsumieren; zum besseren Verständnis werden nachfolgend die Dienstleistungen getrennt nach den einzelnen Bereichen zusammenfassend beschrieben.

**Kauf/Verkauf von Immobilien:** im Rahmen der Tätigkeit sowohl nach § 1 NO als auch § 5 NO wirken Notare am Erwerb von Immobilien ihrer Auftraggeber (Rechtsberatung, Vertragserrichtung, Unterschriftsbeglaubigung, grundbücherliche Durchführung, steuerrechtliche Gebührenbemessung und -einhebung) mit. Dieses notarielle Geschäftsfeld umfasst 28,8 % der Tätigkeit (siehe oben Punkt 1.2. a.).

**Kauf/Verkauf von Unternehmen:** im Rahmen der Tätigkeit sowohl nach § 1 NO als auch § 5 NO wirken Notare am Erwerb von Unternehmen für ihre Auftraggeber mit (Rechtsberatung, Vertragserrichtung, Unterschriftsbeglaubigung, steuerrechtliche Gebührenbemessung und -einhebung). Insgesamt beläuft sich der Anteil dieser notariellen Dienstleistung auf 6,6 % (vergleiche oben Punkt 1.2.b.).

**Verwaltung von Geld, Wertpapieren oder sonstigen Vermögenswerten:** die Verwaltung von Geld, Wertpapieren und sonstigen Vermögenswerten durch Notare ist im Rahmen von § 5 NO grundsätzlich möglich, jedoch selten, was der diesbezügliche geringe Anteil von 2,1 % an den notariellen Tätigkeiten zeigt (vergleiche oben Punkt 1.2.c., d. und e.). In der Praxis erfolgt die Verwaltung von Geld, Wertpapieren und sonstigen Vermögenswerten durch den Notar überwiegend (mit 1,5 % Anteil) als gerichtlich bestellter Kurator oder im Rahmen der Tätigkeit als (gerichtlicher) Erwachsenenvertreter bzw. Vorsorgebevollmächtigter für nicht-entscheidungsfähige Personen.

**Eröffnung oder Verwaltung von Bank-, Spar- oder Wertpapierkonten:** die Eröffnung von Bankkonten ist insbesondere im Zusammenhang mit dem Kauf/ Verkauf von Immobilien und Kauf/Verkauf von Unternehmen möglich, wobei die Konten in diesen Fällen immer Treuhandkonten (Anderkonten) für die Abwicklung der jeweiligen Transaktion sind. Für diese Konten, die nur bei einem speziell dafür anerkannten Kreditinstitut (siehe dazu oben Punkt 2.2.1) geführt werden dürfen, gibt es ein engmaschiges berufs- und aufsichtsrechtliches Netz. Darüberhinausgehend ist eine Eröffnung oder Verwaltung von Bank-, Spar- oder Wertpapierkonten im Rahmen der Verwaltung von Geld, Wertpapieren oder sonstigen Vermögenswerten möglich. Es handelt sich diesfalls regelmäßig um Konten, die als Kurator oder gerichtlicher Erwachsenenvertreter geführt werden und daher einer gerichtlichen Kontrolle unterliegen. Schließlich ist die Eröffnung eines Bankkontos im Rahmen der Verwahrung von Geld (§ 5 und § 104ff NO) möglich. Konten gemäß § 104 NO (diese könnten nur aus Anlass der Aufnahme einer Notariatsurkunde zur Verwahrung von Geld und anschließender Ausfolgung im Parteienauftrag an einen bestimmten Empfänger oder zum Erlage bei Behörden bzw. bei Gericht eingerichtet werden) werden in der Regel zum Erlage bei Gericht eröffnet und sind daher für Täter uninteressant. Sie spielen in der Praxis kaum eine Rolle. Außerhalb der genannten Punkte gibt es regelmäßig keine Beteiligung von Notaren bei Eröffnung oder Verwaltung von Bank-Spar- oder Wertpapierkonten.

**Gründung, Betrieb, Verwaltung von Trusts, Gesellschaften, Stiftungen oder ähnlichen Strukturen einschließlich Beschaffung der zur Gründung, zum Betrieb oder zur Verwaltung von Gesellschaften erforderlichen Mittel:** „Trusts“ sind der österreichischen Rechtsordnung fremd. In Österreich gibt es Stiftungen nach dem Privatstiftungsgesetz (PSG). Gemäß § 1 Abs. 1 PSG sind Privatstiftungen Rechtsträger, denen vom Stifter ein Vermögen gewidmet ist, um durch dessen Nutzung, Verwaltung und Verwertung der Erfüllung eines erlaubten, vom Stifter bestimmten Zwecks zu dienen; sie genießen Rechtspersönlichkeit und müssen ihren Sitz im Inland haben. Privatstiftungen sind auch zwingend im Firmenbuch und im Register der wirtschaftlichen Eigentümer einzutragen. Im Rahmen der Tätigkeit sowohl nach § 1 NO als auch § 5 NO wirken Notare (auch aufgrund gesetzlicher Formvorschriften) an der

Gründung von Gesellschaften und Stiftungen für ihre Auftraggeber mit (Rechtsberatung, Errichtung und gegebenenfalls Änderung der Gesellschaftsverträge, Antragstellungen beim Firmenbuch, Mitwirkung an allfälligen Umstrukturierungen). Insgesamt beträgt der Anteil dieser Tätigkeit 9,7 % (vergleiche oben Punkt 1.2. f., g. und h.).

Üblicherweise erfolgen keine Tätigkeiten von Notaren im Rahmen der Verwaltung oder dem Betrieb von Gesellschaften oder ähnlichen Strukturen. Notare sind auch nicht in die Beschaffung der zur Gründung, zum Betrieb oder zur Verwaltung von Gesellschaften bzw. ähnlichen Strukturen erforderlichen Mittel involviert.

## Bedrohung

### **Terrorismusfinanzierung:**

In den zusammengefassten Szenarien der SNRA wird die Bedrohung durch Missbrauch der legal services sowohl für den Bereich der Terrorismusfinanzierung als auch für den Bereich der Geldwäscherei aufgrund festgestellter Methoden zur Verschleierung des illegalen Ursprungs finanzieller Mittel generell als sehr hoch (very significant) eingestuft (vgl SNRA SWD (2019) 650, Seite 183). Diese Beurteilung scheint nicht stichhaltig, da zwar bei Geldwäscherei die betroffenen Vermögenswerte stets durch strafbare Handlungen (Vortaten) erlangt werden, bei Terrorismusfinanzierung die Vermögenswerte aber sowohl aus legalen als aus illegalen Quellen stammen können (und entsprechend vor allem die Mittelverwendung im Fokus steht). Eine differenzierte, nach den Bereichen Terrorismusfinanzierung / Geldwäscherei und geldwäschegeneigten Geschäften im Sinne Art. 2 Abs. 1 Z 3 lit. b der Richtlinie (EU) 2018/843 und der Notariatsordnung getrennte Betrachtung ist daher sinnvoll und wird nachstehend vorgenommen.

Bei allen geldwäschegeneigten Geschäftsbereichen besteht die **Bedrohung** des Missbrauchs für Terrorismusfinanzierung darin, dass durch Beiziehung eines Notars bzw. Abwicklung des Geschäfts über den Notar Unbedenklichkeit, Seriosität und Bonität suggeriert werden könnte. Wenn Bankkonten involviert sind, könnte zudem die Gefahr bestehen, dass Banken Notare als Kontoinhaber weniger streng überprüfen.

**Klassisches Bedrohungsszenario** könnte beim **Kauf/Verkauf von Immobilien** der Versuch von Tätern sein, durch Investitionen im Immobiliensektor Vermögenswerte für Zwecke der Terrorismusfinanzierung zu lukrieren (zB durch gewinnbringende Investitionen).

**Klassisches Bedrohungsszenario** könnte beim **Kauf/Verkauf von Unternehmen** der Versuch von Tätern sein, durch Investitionen in Unternehmen Vermögenswerte für Zwecke der Terrorismusfinanzierung zu lukrieren (zB durch gewinnbringende Investitionen).

**Klassisches Bedrohungsszenario** könnte bei der **Verwaltung von Geld, Wertpapieren oder sonstigen Vermögenswerten** der Versuch von Tätern sein, Notare als „Stroh Männer“ bei der Verwaltung von Vermögen für Zwecke der Terrorismusfinanzierung einzusetzen.

**Klassisches Bedrohungsszenario** bei der **Eröffnung oder Verwaltung von Bank-, Spar- oder Wertpapierkonten** könnte im Bereich der Terrorismusfinanzierung die Eröffnung von Spendenkonten als Deckmantel zur Sammlung von Geldern sein.

**Klassisches Bedrohungsszenario** bei **Gründung, Betrieb, Verwaltung von Trusts, Gesellschaften, Stiftungen oder ähnlichen Strukturen einschließlich Beschaffung der zur Gründung, zum Betrieb oder zur Verwaltung von Gesellschaften erforderlichen Mittel** könnte der Versuch von Tätern sein, aus zu gründenden Gesellschaften Geld zu lukrieren, das in weiterer Folge zu Zwecken der Terrorismusfinanzierung verwendet werden soll.

**Conclusio:**

**Zusammenfassend ist die Bedrohung im Bereich der Terrorismusfinanzierung als niedrig (lowly significant) einzustufen.**

**Geldwäscherei:**

Bei allen geldwäschegeneigten Geschäftsbereichen besteht die **Bedrohung** des Missbrauchs für Geldwäscherei darin, dass durch Beiziehung eines Notars bzw. Abwicklung des Geschäfts über den Notar Unbedenklichkeit und Seriosität suggeriert werden könnte. Wenn Bankkonten involviert sind, könnte zudem die Gefahr bestehen, dass Banken Notare als Kontoinhaber weniger streng überprüfen.

**Klassisches Bedrohungsszenario** könnte beim **Kauf/Verkauf von Immobilien** im Geldwäschebereich der Versuch von Tätern sein, durch Investitionen im Immobiliensektor die Herkunft widerrechtlich erlangter Vermögenswerte zu verschleiern. Insbesondere bei hochpreisigen Immobilien könnte „mit einem Schlag“ der illegale Ursprung hoher Erträge aus kriminellen Aktivitäten verschleiert und damit „sauber gewaschen“ werden.

**Klassisches Bedrohungsszenario** könnte beim **Kauf/Verkauf von Unternehmen** im Geldwäschebereich der Versuch von Tätern sein, durch den Erwerb von Unternehmen die Herkunft widerrechtlich erlangter Vermögenswerte zu verschleiern. Insbesondere bei betragsmäßig hohen Unternehmenskäufen könnte „mit einem Schlag“ der illegale Ursprung hoher Erträge aus kriminellen Aktivitäten verschleiert und damit „sauber gewaschen“ werden. Durch derartige Investitionen könnte auch die Bonität erworbener Unternehmen für weitere kriminelle Handlungen genutzt werden (zB durch Kreditaufnahmen).

**Klassisches Bedrohungsszenario** könnte bei der **Verwaltung von Geld, Wertpapieren oder sonstigen Vermögenswerten** der Versuch von Tätern sein, Notare als „Strohänner“ bei der Verwaltung von Vermögen zur Mittelherkunftsverschleierung im Bereich der Geldwäscherei einzusetzen.

**Klassisches Bedrohungsszenario** bei der **Eröffnung oder Verwaltung von Bank-, Spar- oder Wertpapierkonten** könnte im Bereich der Geldwäscherei der Versuch sein, Notare als Finanzagenten zu missbrauchen, indem sie über Konten finanzielle Transaktionen tätigen, um den illegalen Ursprung der Gelder zu verschleiern.

**Klassisches Bedrohungsszenario** bei **Gründung, Betrieb, Verwaltung von Trusts, Gesellschaften, Stiftungen oder ähnlichen Strukturen einschließlich Beschaffung der zur Gründung, zum Betrieb oder zur Verwaltung von Gesellschaften erforderlichen Mittel** könnte im Bereich der Geldwäscherei der Versuch von Tätern sein, inkriminierte Vermögenswerte für die Gründung von Entitäten zu verwenden, um damit die illegale Herkunft zu verschleiern.

**Conclusio:**

**Zusammenfassend ist die Bedrohung im Bereich der Geldwäscherei als mittel bis hoch (moderately significant bis significant) einzustufen.**

**Verletzbarkeit**

In den zusammengefassten Szenarien der SNRA wird die Verletzbarkeit der legal services für den Bereich der Terrorismusfinanzierung und den Bereich der Geldwäscherei einheitlich als hoch (significant) eingestuft. Da im Notariatsbereich bezüglich Risikopotential, Risikobe-

wusstsein und rechtlichen Rahmenbedingungen/Aufsicht/Governance keine inhaltlichen Unterschiede bestehen, wird bei der Verletzbarkeit – wie in der SNRA – eine einheitliche Einschätzung vorgenommen.

**(a) Risikopotential:** In den Bereichen Kauf/Verkauf von Immobilien und Kauf/Verkauf von Unternehmen wird jährlich eine hohe Anzahl von Transaktionen mit teils hohen Volumina durch Notare abgewickelt (siehe oben Punkt 2.2.1, Seite 3) abgewickelt. Zudem steigen derzeit durch die COVID 19 Pandemie die Immobilienpreise teils stark. Insgesamt ist Österreich bei Kriminellen auch wegen humaner Haftbedingungen „beliebt“, was das Risiko krimineller Aktivitäten verstärken könnte.

**(b) Risikobewusstsein:** Es besteht ein hohes Risikobewusstsein im gesamten Berufsstand (Notare, Notariatskandidaten, Mitarbeiter und Kammern), was insbesondere auf die Vielzahl risikomindernder Maßnahmen zurückzuführen ist: jeder Notar ist zur Erstellung und laufenden Aktualisierung einer persönlichen Risikoanalyse verpflichtet. Auch die ÖNK erstellt regelmäßig eine sektorale Risikoanalyse für den Bereich des Notariats, die ebenso wie die Nationale und SNRA in die persönliche Bewertung des Notars miteinfließen. Die ÖNK und die Notariatskammern als Aufsichtsbehörden setzen umfassende Maßnahmen im Bereich der Schulung und Sensibilisierung (Seminare, ausführliche und laufend aktualisierte Guidance, Informationsschreiben, Informationsangebot auf der Webseite notar.at, etc). Es erfolgen regelmäßige und effektive Aufsichtsmaßnahmen durch die Notariatskammern (Kanzleirevisionen gemäß § 154 NO), bei denen insbesondere die Einhaltung der Geldwäsche- / Terrorismusfinanzierungspflichten geprüft werden. Im Falle festgestellter Verstöße gegen berufsrechtliche Vorschriften gibt es strenge disziplinarrechtliche Konsequenzen (vgl § 158 NO). Zudem ist in diesem Bereich insbesondere auf die mit der Abwicklungstreuhanderschaft (eine solche gibt es praktisch in jedem Fall einer Immobilientransaktion und in den meisten Fällen einer Unternehmenstransaktion) verbundenen Sicherungsinstrumente (Treuhandregister, Abwicklung über ein anerkanntes Kreditinstitut gemäß § 109a NO). Siehe zu allem näher oben Punkte 2.2.1 und 2.2.2, Seite 3f.

**(c) Rechtlichen Rahmenbedingungen und Aufsicht/Governance:** Zusätzlich ist zu beachten, dass in Österreich bei den notariellen Dienstleistungen außer dem Notar weitere zur Prävention von Geldwäscherei und Terrorismusfinanzierung Verpflichtete Berufsgruppen, Behörden und Gerichte involviert sind. Beispielsweise erfolgt bei Immobilientransaktionen vor Eintragung im gerichtlich geführten Grundbuch eine Prüfung der zugrundeliegenden Titel (Urkunden) durch die Grundbuchgerichte (§ 26 GBG). Die Finanzbehörden sind mit ihren Prüfmechanismen insbesondere als Registerbehörde des Registers der wirtschaftlichen Eigentümer und durch die Berechnung und Abführung von Steuern und Gebühren (ImmoEST, GrEST, Eintragungsgebühr) beteiligt. Soweit eine Selbstberechnung durch Notare vorgenommen wird, erfolgt diese im Interesse der Finanzverwaltung und wird von dieser auch im Wege von besonderen Betriebsprüfungen nachgeprüft; die Notare übernehmen hier quasi eine Inkassofunktion für die Republik Österreich. Bei Immobilientransaktionen mit Käufern aus Drittstaaten (Ausländergrunderwerb) erfolgt außerdem eine Prüfung des wirtschaftlichen Eigentümers durch die Behörden.

Bei jeder Zahlung über Konten ist eine Bank beteiligt, die ihrerseits den strengen Vorschriften des FM-GwG unterliegt. Bei notariellen Transaktionen gibt es zudem ein strenges Anerkennungsverfahren, bei welchen Banken Notare Konten führen und Klientengelder erlegen dürfen. Derzeit ist nur die Notartreuhandbank (NTB), die neben sonstigen Sicherungsmaßnahmen ein taggleiches Verständigungssystem aller an einer Transaktion Beteiligten einzuhalten hat.



#### **Human- und Finanzressourcen:**

In der ÖNK, den sechs Notariatskammern und dem Ständigen Büro in Brüssel haben 2020 insgesamt 157 Personen mit der Thematik Prävention von Terrorismusfinanzierung und Geldwäscherei sowie Aufsicht im Zusammenhang mit der Prävention von GW/TF zu tun.

#### **Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine hohe Verletzbarkeit (significant) nahelegen, führen die dargelegten nationalen und (für die Bereiche Terrorismusfinanzierung und Geldwäscherei identen) berufsinternen Rahmenbedingungen dazu, dass die Verletzbarkeit von Notaren, für Zwecke der Terrorismusfinanzierung oder Geldwäscherei missbraucht zu werden, mit mittel bis hoch einzustufen ist.**

#### **Risikomindernde Maßnahmen**

Zusätzlich zu den oben unter Risikobewusstsein bereits genannten risikomindernden Maßnahmen sind folgende zukünftige Maßnahmen zu nennen, die das Risiko auch pro futuro weiter mindern:

- Der risikobasierte Ansatz bei den Aufsichtsmaßnahmen der Notariatskammern wird weiter verstärkt (zB Risikoklassifizierung der Notare durch technischen Risikomonitor, On-site und Off-site visits), indem bei der ÖNK eine zentrale Stabstelle zur Koordinierung der Geldwäsche-/Terrorismusfinanzierungs-Aufsichtsmaßnahmen durch die Notariatskammern eingerichtet wird. Die persönlichen Risikoanalysen werden verstärkt überprüft.
- Die aus der risikobasierten Aufsicht gewonnenen Erkenntnisse fließen verstärkt in die Aus- und Fortbildung ein; spezielle Revisoren-Schulungen sollen Standard werden.
- Das BMF hat ausländische Rechtsträger (Gesellschaften, Stiftungen und vergleichbare juristische Personen, deren Sitz sich nicht im Inland oder einem anderen Mitgliedstaat befindet) in den Anwendungsbereich des WiEReG einbezogen. Wollen diese ausländischen Rechtsträger Eigentum an einem im Inland gelegenen Grundstück erwerben, gelten sie als meldepflichtige ausländische Rechtsträger, die sich vor der Beurkundung oder Aufnahme einer Notariatsurkunde zum Zwecke des Erwerbs eines im Inland gelegenen Grundstücks in das Ergänzungsregister für sonstige Rechtsträger einzutragen und danach ihre wirtschaftlichen Eigentümer zu melden haben. Notare müssen künftig vor der Beurkundung oder Aufnahme einer Notariatsurkunde zum Zwecke eines Erwerbs eines im Inland gelegenen Grundstücks durch meldepflichtige ausländische Rechtsträger sowie Trusts und trustähnliche Vereinbarungen, deren Verwaltung sich nicht im Inland oder in einem anderen Mitgliedstaat befindet, vergewissern, dass diese ihre wirtschaftlichen Eigentümer gemeldet haben. Die Pflichten der betreffenden Rechtsträger sind mit hohen Strafen (Finanzvergehen bis zu EUR 200.000) sanktioniert.
- Die verstärkte Kooperation (Amtshilfe) zwischen ÖNK/Notariatskammern und anderen Stakeholdern im Bereich der Prävention von Geldwäscherei oder Terrorismusfinanzierung wird das Risiko weiter mindern. Insbesondere besteht eine PPP mit dem BMI/Geldwäsche-Meldestelle (A-FIU), die beispielsweise den Notaren Zugang zu aktuellen Informationen über Methoden und Anhaltspunkte der Kriminellen zu verschaffen und Notaren eine zeitgerechte Rückmeldung in Bezug auf die Wirksamkeit von Verdachtsmeldungen und die daraufhin getroffenen Maßnahmen zu geben hat (§ 37 Abs. 9 NO).



### Gesamtrisiko

Unter Berücksichtigung der bereits bestehenden (siehe Punkt Risikobewusstsein) und der zukünftigen risikomindernden Maßnahmen ist das Gesamtrisiko für Terrorismusfinanzierung als niedrig bis mittel (lowly significant bis moderately significant) und für Geldwäsche als mittel (moderately significant) einzustufen.

### Empfehlungen

- Weiterführung der verstärkten Kooperation zwischen dem Notariat und anderen beteiligten Behörden, insbesondere BMJ, BMF und BMI/ Geldwäsche-Meldestelle.
- Weiterführung der Schulung und Sensibilisierung des Berufsstandes.
- Ausbau der risikobasierten Aufsicht, Einrichtung einer Stabstelle bei der ÖNK und Schulung der Revisoren, um das notwendige berufsinterne know how mit fachspezifischem know how zu Prävention und Erkennung von Geldwäsche oder Terrorismusfinanzierung abzurunden.

# Sektorrisikoanalyse

## Wirtschaftstreuhandberufe

### Steuerberatung und Wirtschaftsprüfung

#### Allgemeine Informationen

Die Berufsgruppen der Steuerberater und Wirtschaftsprüfer fallen als freie Berufe im Bereich der wirtschaftlichen und rechtlichen Beratung und Vertretung in die Kategorie des Nicht-Finanzsektors. Steuerberatern und Wirtschaftsprüfern kommt in Bezug auf die Prävention von Geldwäsche und Terrorismusfinanzierung vor allem eine indirekte „Beobachterrolle“ zu, da sie nur selten direkt an Finanztransaktionen beteiligt sind. Eine direkte Rolle bei Finanztransaktionen kommt ihnen dabei größtenteils nur bei der Übernahme von Treuhandschaften zu, was jedoch nicht zur Kerntätigkeit dieser Berufsgruppen zählt.

Durch ihre Tätigkeiten und Dienstleistungen können sie aber detaillierte Einblicke in die Strukturen und Finanzen ihrer Klienten bekommen. Dies vor allem in Hinblick auf Unternehmen. So ist es Steuerberatern und Wirtschaftsprüfern teilweise möglich sich ein Bild über die Herkunft der Einnahmen sowie der wirtschaftlich Berechtigten zu verschaffen und eventuell können etwaige Auffälligkeiten erkannt werden. Damit kann auch ihnen eine wichtige Rolle im Bereich der Verhinderung von Geldwäsche und Terrorismusfinanzierung zukommen. Gemäß § 77 Abs. 6 WTBG 2017 sind Steuerberater und Wirtschaftsprüfer berechtigt, die ihnen erteilten Auskünfte und übergebenen Unterlagen des Auftraggebers, insbesondere Zahlenangaben, als richtig und vollständig anzusehen. Prüfungsaufträge und andere Aufträge, die zur Unparteilichkeit und Unabhängigkeit verpflichten, dürfen nur nach gewissenhafter Erhebung des Zutreffens der zu bestätigenden Tatsachen und Umstände ausgeführt werden.

#### Anzahl der Berufsträger und Gesamtumsatz

Mit Stand Jänner 2020 gibt es in Österreich insgesamt 11.052 Berufsbefugnisträger in den Bereichen Steuerberatung und Wirtschaftsprüfung.

Dies lässt sich weiter auf 7.898 natürliche Personen und 3.154 juristische Personen aufteilen.

Insgesamt gibt es in Österreich mit Stand Jänner 2020 8.080 Berufsbefugnisträger im Bereich Steuerberatung, davon sind 5.915 natürliche Personen und 2.165 juristische Personen.

Insgesamt gibt es in Österreich mit Stand Jänner 2020 2.972 Berufsbefugnisträger im Bereich Wirtschaftsprüfung, davon sind 1.983 natürliche Personen und 989 juristische Personen.

Der ermittelte Gesamtumsatz aller Steuerberater und Wirtschaftsprüfer in Österreich betrug mit Stand 2019 rund 2,8 Mrd. Euro.

#### Kanzleistruktur

Steuerberater und Wirtschaftsprüfer bedienen sich in der Ausübung ihrer Tätigkeiten verschiedenster Kanzleistrukturen. Diese reichen von kleinen Ein-Personen-Kanzleien bis hin zu großen Kanzleinetzwerken mit bis zu über 1.000 Mitarbeitern. Mitarbeiter sind dabei nicht nur Berufsberechtigte und Berufsanwärter, sondern auch Personen, welche Front- und

Back-Office-Tätigkeiten übernehmen oder organisatorisch und systemerhaltend in den Kanzleien agieren.

Die Größe der Kanzleien in Österreich gliedert sich nach der Anzahl der Mitarbeiter mit Stand 2019 wie folgt:

- rund 70% - Kanzleien mit weniger als zehn Mitarbeitern
- rund 26% - Kanzleien mit 10 – 50 Mitarbeitern
- rund 4% - Kanzleien mit 50 – über 500 Mitarbeitern.

#### **Anzahl der Auftraggeber**

Steuerberater und Wirtschaftsprüfer werden größtenteils für eine Vielzahl von Auftraggebern tätig. Auftraggeber sind einerseits Privatpersonen aus allen beruflichen Bereichen und andererseits bzw. vor allem auch Unternehmen aus den verschiedensten wirtschaftlichen Sparten.

Die Anzahl der Auftraggeber pro Kanzlei verteilt sich statistisch in Österreich mit Stand 2019 wie folgt:

- rund 41% der Kanzleien betreuen bis zu 100 Mandanten,
- rund 42% betreuen bis zu 500 Mandanten,
- rund 11% betreuen bis zu 1.000 Mandanten,
- und rund 6% der Kanzleien betreuen sogar mehr als 1.000 Mandanten.

#### **Verschwiegenheitspflicht (legal privilege)**

Steuerberater und Wirtschaftsprüfer unterliegen aufgrund des streng vertraulichen Verhältnisses zu ihren Mandanten in Rahmen ihrer beruflichen Tätigkeit einer Verschwiegenheitspflicht. Die exakte Bestimmung und Ausgestaltung dazu befindet sich in § 80 WTBG 2017. Diese Verschwiegenheitspflicht entfällt jedoch gemäß § 80 Abs. 4 WTBG 2017 wenn und insoweit Melde- und Auskunftspflichten im Rahmen der Bestimmungen der Richtlinie (EU) 2018/843 und den damit im Zusammenhang erlassenen Umsetzungsmaßnahmen bestehen.

#### **Bedrohung**

##### **Geldwäscherei und Terrorismusfinanzierung:**

Wie auch in der SNRA weist die KSW darauf hin, dass die Bewertung der terroristischen Bedrohung im Zusammenhang mit Dienstleistungen von Wirtschaftsprüfern und Steuerberatern zusammen mit Geldwäscherei geprüft wurde. Die Bedrohung durch die Terrorismusfinanzierung bedarf daher keiner gesonderten Bewertung.

In den zusammengefassten Szenarien der SNRA wurde die Bedrohung, dass Steuerberater und Wirtschaftsprüfer für Geldwäscherein und terroristische Aktivitäten missbraucht zu werden, mit einem signifikanten Risiko eingestuft. In der Folge soll die nationale Bedrohung abgeleitet werden.

Wie in der SNRA ausgeführt, liegt die Hauptbedrohung bei Steuerberatungs- und Wirtschaftsprüfungsdienstleistungen, ähnlich wie den anderen rechtsberatenden Berufen, in der Infiltration durch oder des Missbrauchs durch die organisierte Kriminalität. Die Berufsberechtigten könnten unabsichtlich an der Geldwäsche dieser Gruppen beteiligt sein, können jedoch auch bei der Erfüllung ihrer Sorgfaltspflichten gegenüber solchem Kunden vorsätzlich oder fahrlässig die gesetzlichen Bestimmungen ignorieren.

Laut der SNRA greifen Gruppen der organisierten Kriminalität häufig auf Steuerberater und Wirtschaftsprüfer zurück, um sich beraten zu lassen und / oder um diese in ihre Geldwäschesysteme einzubeziehen. Die Dienstleistungen von Steuerberatern und Wirtschaftsprüfern werden als nützlich für die Einrichtung von Geldwäschesystemen angesehen, da sie für bestimmte Arten von Aktivitäten benötigt werden und / oder weil der Zugang zu speziellen steuerlichen Fachkenntnissen und Fähigkeiten bei der Geldwäsche hilfreich sein kann. Gemäß SNRA gibt es auch Hinweise, dass einige Kriminelle versuchen, Steuerberater und Wirtschaftsprüfer zu kooptieren und wissentlich in ihre Geldwäschesysteme einzubeziehen. Die Berufsberechtigten können dabei in unterschiedlichem Maße in den Geldwäschereiprozess einbezogen werden. Sie können konsultiert werden, wie bestimmte rechtliche Rahmenbedingungen umgangen und vermieden werden können oder sie können proaktiver vorgehen, indem sie den Geldwäschereiprozess direkt unterstützen oder koordinieren.

Dienstleistungen von Steuerberatern und Wirtschaftsprüfern werden für legitime Zwecke verwendet. Sie können jedoch auch eine Vielzahl von Geldwäschesystemen unterstützen. Die Kammer der Steuerberater und Wirtschaftsprüfer in Österreich hat jedoch keine Anhaltspunkte dafür, dass die Berufsgruppen im großen Stile für Tätigkeiten der Geldwäscherei und Terrorismusfinanzierung missbraucht werden. Die strafrechtlichen Verfolgungen und Verurteilungen, welche der Kammer aufgrund der berufsrechtlichen Bestimmungen gemeldet werden, zeigen, dass nur sehr vereinzelt Berufsberechtigte proaktiv in Geldwäschereisystemen einbezogen sind. Auch anderweitige Statistiken, wie etwa jene der Hausdurchsuchungen bei Steuerberatern und Wirtschaftsprüfern zeigen, dass diese auch nur selten als Betroffene im Rahmen von Geldwäscherei- und Terrorismusfinanzierungssystemen involviert sind.

**Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine signifikante Bedrohung nahelegen, zeigen die aktuellen nationalen Daten, dass im Dienstleistungssektor der Steuerberatung und Wirtschaftsprüfung aufgrund der nationalen Daten und Statistiken, wohl jedenfalls von keiner signifikanten Bedrohung auszugehen ist. Zusammenfassend ist die Bedrohung daher mit mittel einzustufen.**

**Verletzbarkeit**

**Geldwäscherei und Terrorismusfinanzierung:**

Wie auch in der SNRA weist die KSW darauf hin, dass die Bewertung der Verletzbarkeit durch Terrorismusfinanzierung im Zusammenhang mit Dienstleistungen von Wirtschaftsprüfern und Steuerberatern zusammen mit Geldwäscherei geprüft wurde. Die Verletzbarkeit durch die Terrorismusfinanzierung bedarf daher keiner gesonderten Bewertung.

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von Dienstleistung von Steuerberatern und Wirtschaftsprüfern im Hinblick auf den Missbrauch für die Zwecke der Geldwäscherei und Terrorismusfinanzierung signifikant eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden.

**(a) Risikopotential:**

Risiken bestehen primär durch die angebotenen Dienstleistungen der Berufsgruppen. Folglich soll nun ein Überblick über die relevantesten Dienstleistungen der beiden Berufsgruppen und deren Risikopotential gemacht werden:

**Personalverrechnung:**

Diese Dienstleistung bezieht sich auf das Ermitteln von Bezugsansprüchen von Arbeitnehmern, die Ermittlung von Auslagensätzen etc. bis hin zur Betreuung und Vertretung bei Lohnsteuer-, Sozialversicherungs- und Kommunalsteuerprüfung. In Rahmen der Personalverrechnung wird das Risiko der Berufsgruppen für Zwecke der Geldwäscherei und Terrorismusfinanzierung missbraucht zu werden, als gering bis mittel angesehen. Rechtswidriges Verhalten, wie etwa das Umgehen von Schwarzbeschäftigung etc. kann hier durch den Berufsberechtigten zum Teil und mit Verweis auf § 77 Abs. 6 WTBG 2017 erkannt und gemeldet werden.

**Buchhaltung**

Zum Dienstleistungsbereich der Buchhaltung gehört unter anderem das Führen der Buchhaltung aufgrund der vom Klienten zur Verfügung gestellten Unterlagen, das Erstellen und Übermitteln der Umsatzsteuervoranmeldung, das Bereitstellen monatlicher Saldenlisten für Sach- und Personenkonten. Auch hier wird das Risiko der Berufsgruppen für Zwecke der Geldwäscherei und Terrorismusfinanzierung missbraucht zu werden, als gering bis mittel angesehen. Hier können Berufsberechtigte Auffälligkeiten unter Umständen identifiziert und etwaige rechtswidrige Vorgänge gemeldet werden. Durch die Vorlage von gefälschten Belegen oder Umsätzen kann dies aber wesentlich erschwert werden. Auch an dieser Stelle kann auf die eingangs dargelegten Ausführungen zu § 77 Abs. 6 WTBG 2017 verwiesen werden.

**Jahresabschlusserstellung**

Die jährliche Erstellung des Jahresabschlusses stellt eine der Kerntätigkeiten für Steuerberater und Wirtschaftsprüfer dar. Berufsberechtigte sind zumeist in sämtliche Schritte der Erstellung des Jahresabschlusses involviert. Gerade hier veranschaulicht sich auch die bereits oben erwähnte indirekte „Beobachterrolle“ der Berufsberechtigten. Diese sind zwar nicht unmittelbar an den finanziellen und wirtschaftlichen Vorgängen der Unternehmen beteiligt doch erhalten diese im Zuge der Jahresabschlusserstellung genauen Einblick in die finanziellen und wirtschaftlichen Vorgänge von Unternehmen. Steuerberatern und Wirtschaftsprüfern ist es somit möglich Verdachtsmomente in Bezug auf Geldwäsche und Terrorfinanzierung zu erkennen. Diesbezüglich würde sie eine Meldeverpflichtung an die Geldwäschemeldestelle treffen. Das Risiko der Berufsgruppen bei der Jahresabschlusserstellung für Zwecke der Geldwäsche und Terrorfinanzierung missbraucht zu werden, wird hingegen als gering bis mittel angesehen. Nur durch die aktive falsche Erstellung eines Jahresabschlusses durch einen Steuerberater oder eines Wirtschaftsprüfers wäre dies hier wohl möglich.

**Beratung (inkl. Steuererklärung und Gutachtertätigkeit)**

Die beratende Tätigkeit stellt einen weiteren Schwerpunkt der Dienstleistungen von Steuerberatern und Wirtschaftsprüfern dar. Dabei handelt es sich vor allem um Beratungsleistungen im Bereich des Abgabenrechts und der Rechnungslegung, aber auch um Beratungen in Zusammenhang mit arbeitstechnischen Fragen, in Beitrags-, Versicherungs- und Leistungsangelegenheiten der Sozialversicherungsträger sowie im Bereich der Sanierungsberatung. Des Weiteren werden noch weitere Beratungsgebiete in den §§ 2 und 3 des WTBG 2017 genannt, welche auch vereinzelt wahrgenommen werden. In den meisten dieser Beratungsbereiche sind die Berufsberechtigten auch zu Vertretung befugt. So z.B. im Abgaben- und Abgabenstrafverfahren. Auch werden in diesem Zusammenhang Gutachten zu komplexen abgabenrechtlichen Fragen erstellt.

Eine weitere Haupttätigkeit in diesem Zusammenhang ist die Erstellung der regelmäßigen Steuererklärungen für die Klienten.

Auch hier kann ähnlich wie bei den Ausführungen zum Tätigkeitsbereich der Jahresabschluss-Erstellung argumentiert werden. Auch hier kommt es vor allem zu einer indirekten „Beobachterrolle“ der Berufsberechtigten. Diese sind nicht unmittelbar an den finanziellen und wirtschaftlichen Vorgängen der Klienten beteiligt, doch erhalten diese im Zuge ihrer Tätigkeiten eventuell Einblick in deren finanzielle und wirtschaftliche Vorgänge. Steuerberatern und Wirtschaftsprüfern ist es somit möglich Verdachtsmomente in Bezug auf Geldwäsche und Terrorfinanzierung zu erkennen. Diesbezüglich würde sie eine Meldeverpflichtung an die Geldwäschemeldestelle treffen. Das Risiko der Berufsgruppen bei Beratungstätigkeiten für Zwecke der Geldwäsche und Terrorfinanzierung missbraucht zu werden, wird hingegen als gering bis mittel angesehen.

#### **Treuhänderische Tätigkeit**

Steuerberater und Wirtschaftsprüfer werden in Rahmen ihrer beruflichen Tätigkeit vereinzelt auch treuhänderisch tätig. Dabei handelt es sich zumeist um eine treuhänderische Tätigkeit in Zusammenhang mit der Abwicklung einer Transaktion bzw. Halten von Beteiligungen. Da hier Berufsberechtigte direkt für ihre Mandanten Finanztransaktionen durchführen, wird hier das Risiko der Berufsberechtigten für Zwecke der Geldwäsche und Terrorfinanzierung missbraucht zu werden mit mittel bis hoch angesehen. Hier sei jedoch darauf verwiesen, dass solcherart durchgeführte Finanztransaktionen ausschließlich unter Einbeziehung von Banken bzw. Finanzinstituten abgewickelt werden, welche ihrerseits wiederum an die strengen Maßnahmen zur Verhinderung der Geldwäsche und Terrorfinanzierung gebunden sind. Diesbezüglich kommt es daher einerseits zu einer Kontrolle durch den Steuerberater/Wirtschaftsprüfer und andererseits durch die jeweilige Bank bzw. das jeweilige Finanzinstitut. Des Weiteren wird die treuhänderische Tätigkeit nur vereinzelt von Steuerberatern und Wirtschaftsprüfern in Österreich wahrgenommen und stellt im Verhältnis zu anderen Tätigkeiten einen eher unwesentlichen Bereich dar.

#### **Prüfungsleistungen**

Bei den Prüfungsleistungen werden einerseits gesetzlich verpflichtende und freiwillige Abschlussprüfungen als auch sonstige gesetzliche Prüfungen und sonstige Prüfungsaufträge wahrgenommen. Hier wird ebenfalls ein geringes bis mittleres Risiko angenommen. Berufsberechtigte, welche gesetzliche Abschlussprüfungen durchführen, werden im Rahmen der regelmäßigen Qualitätssicherungsprüfungen der Abschlussprüferaufsichtsbehörde (siehe unten) kontrolliert und auf die Einhaltung der Maßnahmen zur Verhinderung der Geldwäsche und Terrorfinanzierung geprüft.

Weiters lässt sich das Risikopotential am geografischen Risiko und am Auftragsgeberrisiko festlegen.

#### **Geografisches Risiko**

Steuerberater und Wirtschaftsprüfer erbringen ihre Dienstleistungen größtenteils innerhalb Österreichs. Vor allem kleine Kanzleien und Kanzleien im ländlichen Bereich betreuen dabei meist nur Auftraggeber aus der regionalen Umgebung. Im Gegensatz dazu gibt es Großkanzleien, welche durchaus auch grenzüberschreitend tätig werden. Dabei handelt es sich zumeist um Kanzleien welche Teil eines internationalen Netzwerkes sind (als Beispiel seien die „Big Four“-Unternehmen genannt). Grenzüberschreitende Tätigkeiten sind dabei primär auf Auftraggeber der EU-Mitgliedstaaten ausgerichtet. Wesentlich seltener kommt es zu Dienstleistungserbringung für Auftraggeber aus Drittstaaten. Vereinzelt werden auch Auftraggeber aus Risikoländern betreut.

Statistisch ergibt sich dabei folgende geografische Verteilung bei den betreuten Auftraggebern:

- rund 85% inländische Auftraggeber
- rund 10% Auftraggeber aus EU-Mitgliedstaaten
- rund 5% Auftraggeber aus Nicht-EU-Mitgliedstaaten.

Das geografische Risiko bei Dienstleistungen von Steuerberatern und Wirtschaftsprüfern wird daher durch die KSW als gering bis mittel eingestuft. Sollten Auftraggeber aus Risikoländern betreut werden, so sind die Berufsberechtigten verpflichtet in Rahmen der Maßnahmen zur Verhinderung der Geldwäsche und Terrorismusfinanzierung erhöhte Sorgfaltspflichten anzuwenden – siehe Ausführungen zu den risikominimierenden Maßnahmen.

### **Auftraggeberrisiko**

Wie bereits zuvor erwähnt, werden Steuerberater und Wirtschaftsprüfer für ein weites Spektrum an Auftraggebern tätig. Dabei kann es sich um Einzelpersonen und Ein-Mann-Gesellschaften bis hin zu großen und komplexen Unternehmen und Netzwerken handeln. Weiters werden Berufsberechtigte zum Teil auch für öffentlich-rechtliche Institutionen sowie Gemeinden und Kirchen tätig.

Auch die wirtschaftlichen Branchen der Auftraggeber sind dadurch breit gefächert. Sie umfassen u.a. (Finanz-)Dienstleistungsunternehmen, Handelsunternehmen sowie auch Bauunternehmen udgl.

Aus diesem Grund muss im Bereich des Auftraggeberrisikos von einem mittleren Risiko ausgegangen werden. Eine konkrete Bestimmung des Geldwäsche- und Terrorismusfinanzierungsrisikos eines Auftraggebers bedarf zumeist einer Einzelfallbeurteilung durch den jeweiligen Steuerberater/Wirtschaftsprüfer im Rahmen der verpflichtenden Risikobeurteilung.

Ein erhöhtes Risiko wird jedoch bei bestimmten Auftraggebern indiziert. Dies zum Beispiel, wenn es sich bei der Person des Auftraggebers um einen PEP handelt oder diese ein Familienmitglied eines PEPs oder eine diesem nahestehende Person ist.

Auch gewisse Branchen können ein vermeintlich erhöhtes Risiko indizieren. Dazu gehören vor allem bargeldintensive Branchen (insbesondere z.B. Gastronomie-, Hotel-, Bordell-, Glücksspielbetriebe u.a.), Unternehmen aus dem Bereich Baugewerbe und Bauträger, als auch Immobilienhandel sowie Handel mit hochwertigen Gütern (insbesondere z.B. mit Edelmetallen, Edelsteinen, Schmuck, Uhren, Kunstgegenständen, Antiquitäten, Kraftfahrzeugen, Schiffen, Motorbooten, Luftfahrzeugen, Maschinen u.a.) und Import-/Exportunternehmen.

Es gibt jedoch auch Umstände, welche auf Seiten des Auftraggebers ein niedriges Geldwäsche- und Terrorismusrisiko indizieren.

Dies betrifft vor allem öffentliche, börsennotierte Unternehmen, die Offenlegungspflichten unterliegen, die Anforderungen an die Gewährleistung einer angemessenen Transparenz hinsichtlich des wirtschaftlichen Eigentümers auferlegen. Weiters wird ein solches niedriges Risiko bei der öffentlichen Verwaltung und öffentlich-rechtlichen Institutionen und Unternehmen indiziert.

**(b) Risikobewusstsein:**

Steuerberater und Wirtschaftsprüfer haben bei der Erbringung ihrer Dienstleistungen stets strenge (berufs-) rechtliche Sorgfaltsmaßstäbe anzuwenden und das allgemeine Berufsethos zu beachten.

Dienstleistungen in den Bereichen Steuerberatung und Wirtschaftsprüfung sind außerdem zumeist auf längerfristige Geschäftsbeziehungen ausgerichtet. Dadurch entsteht auch ein gewisses Vertrauensverhältnis zwischen den Berufsberechtigten und ihren Klienten. Steuerberater und Wirtschaftsprüfer können so die wirtschaftlichen und finanziellen Abläufe ihrer Klienten gut evaluieren und mögliche Risiken erkennen. Vereinzelt kommt es jedoch auch zu kürzeren und einmaligen Dienstleistungen, dies vor allem im Bereich der Beratungstätigkeit.

Des Weiteren sind sie berufsrechtlich gem. § 71 Abs. 3 WTBG 2017 verpflichtet stets ihre beruflichen Kenntnisse auf den neuesten Stand zu halten. Die KSW ist stets dazu bedacht ihre Mitglieder im Bereich Geldwäsche und Terrorfinanzierung zu schulen und informiert zu halten. Dies erfüllt die KSW einerseits selbst durch die Organisation von etwaigen Informationsveranstaltungen und Themenabenden sowie durch den Versand von Newslettern. Zusätzlich können sich Berufsberechtigte auch schriftlich und telefonisch bei der KSW in Hinblick auf Verhinderung von Geldwäsche und Terrorfinanzierung beauskunften lassen. Damit wird das Risikobewusstsein im Berufsstand geschärft.

Die KSW stellt auch regelmäßig Auskunftersuchen und Informationsanfragen an relevante Behörden, wie etwa die A-FIU, um neueste Erkenntnisse in den Bereichen Geldwäscherei und Terrorismusfinanzierung zu erhalten. Diese Erkenntnisse werden sodann mit den Berufsgruppen geteilt.

Abschließend sind Berufsberechtigte verpflichtet ihre Angestellten regelmäßig zu den Themen Geldwäscherei und Terrorismusfinanzierung zu schulen. Diese Schulungen müssen dokumentiert werden und werden seitens der KSW auch geprüft.

Durch diese Maßnahmen kann von einem weiten Risikobewusstsein im Berufsstand in Bezug auf Geldwäscherei und Terrorismusfinanzierung gesprochen werden.

**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Steuerberater und Wirtschaftsprüfer müssen bei der Ausübung ihrer Tätigkeit stets die berufsrechtlichen Bestimmungen und Maßnahmen zur Verhinderung der Geldwäsche und Terrorismusfinanzierung beachten, welche in den §§ 87 – 105 WTBG 2017 festgelegt sind. Zusätzlich zu diesen gesetzlichen Bestimmungen unterliegen Berufsberechtigte außerdem der Verordnung der Kammer der Steuerberater und Wirtschaftsprüfer über die Richtlinie über die Geldwäscheprävention bei Ausübung von WT-Berufen (KSW-GWPRL 2017), welche weitere Maßnahmen, Anordnungen und Spezifikationen vorgibt.

Gem. § 101 WTBG 2017 obliegt es der KSW, als Interessensvertretung der Steuerberater und Wirtschaftsprüfer, die Aufsicht über die Einhaltung der Maßnahmen zur Verhinderung der Geldwäsche und Terrorismusfinanzierung vorzunehmen. Dazu sind im Kammeramt selbst 1,5 Vollzeitbeschäftigte angestellt, welche durch den Ausschuss für Geldwäschepräventions-Aufsicht, bestehend aus 8 Funktionären, und den 21 Experten, welche die Vorortprüfungen vornehmen, unterstützt werden.

**Aufsichtsprüfungen der KSW gem. § 102 WTBG 2017**

Die KSW führt zur Aufsicht über die Einhaltung der Maßnahmen zur Verhinderung der Geldwäsche und Terrorismusfinanzierung regelmäßig Aufsichtsprüfungen bei ihren



Mitgliedern durch. Dabei handelt es sich um anlassunabhängige Prüfungen, welche anhand eines risikobasierten Ansatzes vorgenommen werden. Daneben kann es natürlich auch, im Falle eines konkreten Anlassfalles, zu einer anlassbezogenen Prüfung durch die KSW kommen.

Die anlassunabhängigen Prüfungen werden, wie bereits erwähnt, aufgrund eines risikobasierten Ansatzes durchgeführt. Die konkreten, zu prüfenden Berufsberechtigten werden dabei stichprobenartig ausgewählt. Die Prüfungen können auf zwei verschiedene Arten durchgeführt werden.

Einerseits durch eine Offsite-Prüfung, bei welcher die Bewertung anhand von durch den Berufsberechtigten zur Verfügung gestellte, kanzleiinterne Unterlagen und Informationen durchgeführt wird. Andererseits durch eine Nachschau im Betrieb des Berufsberechtigten einschließlich einer stichprobenmäßigen Nachschau in dessen Auftragsunterlagen. Eine Nachschau hat durch Experten im Sinne des § 103 WTBG 2017 zu erfolgen. Solche Experten kommen aus dem Berufsstand der Steuerberater und Wirtschaftsprüfer und werden der aus dem Kreis der Untersuchungskommissäre gem. § 140 WTBG 2017 oder der Qualitätsprüfer gem. § 26 Abs. 5 APAG ausgewählt. Zusätzliche Voraussetzung ist der Nachweis einer einschlägigen Schulung auf dem Gebiet der Verhinderung der Geldwäsche und der Terrorismusfinanzierung.

#### **Prüfungen im Rahmen der Qualitätssicherungsprüfung**

Berufsberechtigte, die im öffentlichen Register gemäß § 52 APAG eingetragen sind, sind von oben angeführten anlassunabhängigen Prüfungen der KSW ausgenommen. Diese Berufsberechtigten werden jedoch in Rahmen ihrer regelmäßigen Qualitätssicherungsprüfungen durch die Abschlussprüferaufsichtsbehörde (APAB) geprüft. Damit eine einheitliche Vorgehensweise für die anlassunabhängigen Prüfungen der KSW und der APAB gegeben ist, wurde seitens der KSW eine Stellungnahme zur Vorgehensweise bei den Prüfungen erarbeitet. Sollte es zu problematischen Feststellungen durch die APAB kommen, so besteht auch eine Mitteilungspflicht der APAB an die KSW, da die KSW alleinige Aufsichtsbehörde in Rahmen der Verhinderung von Geldwäsche und Terrorismusfinanzierung bleibt. Des Weiteren steht es der KSW auch offen, bspw. bei Vorliegen von Verdachtsmomenten eine anlassbezogene Prüfung bei diesem Berufsberechtigten durchzuführen.

#### **Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine signifikante Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von Steuerberatern und Wirtschaftsprüfern, für die Zwecke der Geldwäsche und Terrorismusfinanzierung missbraucht zu werden, mit mittel einzustufen ist.**

#### **Risikomindernde Maßnahmen**

Die Risikominimierenden Maßnahmen der Steuerberater und Wirtschaftsprüfer sind in den §§ 89 – 100 WTBG 2017 geregelt.

Folgend werden nun einzelne Sorgfaltspflichten aufgezählt, welche für Steuerberater und Wirtschaftsprüfer anzuwenden sind.

#### **Identifikation des Auftraggebers**

Bei einer natürlichen Person als Auftraggeber hat die Identifikation durch einen aktuellen amtlichen Lichtbildausweis zu erfolgen. Dasselbe gilt für die gesetzlichen Vertreter bei nicht natürlichen Personen als Auftraggeber in vertretungsbefugter Anzahl (§ 90 Z 1 WTBG 2017).

Steht für die Identifikation einer natürlichen Person kein aktueller amtlicher Lichtbildausweis zu Verfügung, dann schreibt § 1 Abs. 1 KSW-GWPRL vor, dass die Überprüfung risikobasiert auch auf anderen Quellen beruhen kann. Dabei gelten Auskünfte und Informationen von verlässlichen Gewährspersonen als glaubwürdig. Zu diesen zählen Gerichte und sonstige staatliche Behörden, Steuerberater, Wirtschaftsprüfer und Personen mit vergleichbarer ausländischer Berufsbefugnis, Notare, Rechtsanwälte und Kreditinstitute, sofern sie nicht ihren amtlichen Wirkungsbereich, Sitz oder Wohnsitz in einem Nicht-Kooperationsstaat im Sinne des § 94 Abs. 5 WTBG 2017 haben.

Ist Auftraggeber eine juristische Person, so haben Berufsberechtigte die Identität der vertretungsbefugten Personen in vertretungsbefugter Anzahl festzustellen und in der Regel mit Ausweiseistung zu überprüfen. Die Identität von wirtschaftlichen Eigentümern ist festzustellen, z.B. durch Befragung der gesetzlichen Vertreter des Auftraggebers. Die Eigenschaft als wirtschaftlicher Eigentümer sowie die Identität ist unter Ergreifung risikoorientierter und angemessener Maßnahmen z.B. durch Einsichtnahme in das Firmenbuch oder das Wirtschaftliche Eigentümer Register (WiEReG) zu überprüfen. Die Identifikation des Auftraggebers schließt für Steuerberater und Wirtschaftsprüfer angemessene Maßnahmen ein, um die Eigentums- und Kontrollstruktur des Auftraggebers zu verstehen. Liegt im Einzelfall nur ein geringes potenzielles Risiko vor, dass die Dienste des Berufsberechtigten für Zwecke der Geldwäsche oder Terrorismusfinanzierung missbraucht werden, kann es, wenn auch sonst kein Indiz für ein erhöhtes Risiko dafür vorliegt, ausreichend sein, mit allgemeinen Mitteln ein allgemeines Verständnis der Eigentums- und Kontrollstruktur des Auftraggebers zu erlangen.

Bei sonstigen Vertretern ist neben dem Vertreter auch der Auftraggeber zu identifizieren und sowohl die Identität des Vertreters als auch die aufrechte Vertretungsbefugnis zu überprüfen. § 1 Abs. 3 KSW-GWPRL schreibt dazu die Einholung einer schriftlich erteilten Vollmacht vor; nur bei berufsmäßigen Parteienvertretern genügt die Berufung auf eine erteilte Vollmacht verbunden mit einem Nachweis der Berufsberechtigung.

#### **PEP-Abfrage**

Bei Aufnahme einer neuen Geschäftsbeziehung haben Steuerberater und Wirtschaftsprüfer eine mögliche PEP-Eigenschaft ihres Auftraggebers festzustellen. § 94 Abs. 1 Z 4 WTBG 2017 (Verstärkte Sorgfaltspflichten) stellt klar, dass PEPs, ihre Familienangehörigen und bekanntermaßen nahestehende Personen aus Risikogesichtspunkten gleich zu behandeln sind. Dieser Personenkreis wird in § 87 Abs. 2 Z 14 – 16 WTBG 2017 definiert. Es liegt in der berufsständischen Eigenverantwortung festzulegen, wie überprüft wird, ob ein Auftraggeber oder ein wirtschaftlicher Eigentümer zu diesem Personenkreis zählt. Größtenteils wird dies durch Abfragen in darauf spezialisierten Datenbanken zur diesbezüglichen Überprüfung von Personen, insbesondere hinsichtlich deren Einordnung als politisch exponierte Personen (PEP), durchgeführt.

#### **Kanzleirisikoanalyse**

Der Berufsberechtigte hat alle berufstypischen Tätigkeiten, die in seiner Kanzlei angeboten oder durchgeführt werden, gemäß dem Risiko, für Zwecke der Geldwäsche oder Terrorismusfinanzierung missbraucht werden zu können, auf Basis der Risikoanalysen der EU, der nationalen Risikoanalyse sowie der Risikofaktoren der Anhänge 1 – 3 der 4. GW-RL in eine der Risikokategorien hoch/mittel/gering einzustufen.

### **Kanzleileitfaden**

Der Berufsberechtigte hat gemäß § 88 Abs. 3 WTBG alle zur Erfüllung der GWP-Pflichten verwendeten Strategien und Methoden, ebenso wie dazu verwendete kanzleiinterne Dokumente und Arbeitspapiere sowie der verwendeten Dokumentationssysteme in einem GWP-Kanzleileitfaden zusammenzufassen. Dieser ist allen Mitarbeitern nachweislich zur Kenntnis zu bringen.

Dabei sind Größe und Komplexität der Kanzlei, Dauer und Art der erbrachten Dienstleistung, Person eines Auftraggebers oder eines wirtschaftlichen Eigentümers, Auftragsgeberstruktur und Regionen, in denen der Berufsberechtigte seine Dienstleistungen erbringt, zu berücksichtigen. Ebenso hat der Kanzleileitfaden Informationen über das KSW-Hinweisgebersystem und abhängig von der Kanzleigröße über das kanzleiinterne Hinweisgebersystem zu enthalten. Dieser hat weiters den Ort anzugeben, an dem der aktuell maßgebliche Kanzleileitfaden für Mitarbeitern einsehbar ist sowie eine Klarstellung, wer für die Beantwortung von Fragen dazu zuständig ist. Zusätzlich sollte auf das Einschaurecht der KSW bzw. gegebenenfalls der Abschlussprüferaufsichtsbehörde iZm GWP-Prüfungen hingewiesen werden.

### **Geldwäschebeauftragter**

Berufsberechtigte haben einen besonderen Beauftragten für Fragen der Geldwäsche und Terrorismusfinanzierung einzurichten, wenn dies nach Art und Umfang der Geschäftstätigkeit erforderlich ist (§ 99 Abs. 2 WTBG 2017). Der Berufsberechtigte hat sicherzustellen, dass der Geldwäschebeauftragte jederzeit über ausreichende Berufsqualifikation, Kenntnisse und Erfahrungen verfügt (fachliche Qualifikation) und integer ist (persönliche Zuverlässigkeit).

### **GWP-Dokumentationen**

Inhaltliche Entscheidungen über auftragsabhängige Sorgfaltspflichten sowie deren Basis sind risikobasiert zu dokumentieren. § 98 WTBG (Dokumentations- und Aufbewahrungspflichten) normiert, dass Berufsberechtigte grundsätzlich dazu verpflichtet sind,

1. Unterlagen, die der Erfüllung von Sorgfaltspflichten gegenüber Auftraggebern dienen,
2. Belege und Aufzeichnungen von Transaktionen,
3. Unterlagen, die iZm abgegebenen Verdachtsmeldungen und
4. Unterlagen iZm der Risikoeinstufung des Auftraggebers stehen,

fünf Jahre nach dem letzten Geschäftsfall (bzw. nach der Durchführung der betreffenden Transaktion) aufzubewahren. Die Frist läuft dabei vom Schluss des Kalenderjahres, auf das sich der letzte Geschäftsfall bezieht.

### **Mitarbeiterbestimmungen**

Gemäß § 99 Abs. 1 Z 2 WTBG haben Berufsberechtigte hinsichtlich ihres Personals Sonderpflichten zu erfüllen:

Gemäß § 99 Abs. 1 Z 2 lit. a WTBG 2017 ist Personal bereits bei der Einstellung einer Überprüfung in Bezug auf Geldwäsche oder Terrorismusfinanzierung zu unterziehen. Gemäß § 99 Abs. 1 Z 2 lit. b und c WTBG 2017 sind Mitarbeiter mit den kanzleiinternen Vorschriften nachweislich vertraut zu machen und in besonderen Fortbildungsprogrammen zu schulen. Die Absolvierung der Schulungsmaßnahme sowie der Schulungsinhalt sind jedenfalls zu dokumentieren.

### **Risikoprofil**

Für jeden Auftrag ist zur Beurteilung des Risikos der Geldwäsche oder Terrorismusfinanzierung ein Risikoprofil zu erstellen. Für jeden Auftrag hat der Berufsberechtigte ein Risikoprofil anhand aller über Auftraggeber, Dienstleistung und das Kanzleirisiko und damit zusammenhängenden erhaltenen Informationen zu erstellen und für die Dauer einer Geschäftsbeziehung aktuell zu halten. Bezüglich des Dienstleistungsrisikos ist dabei die Einschätzung in der Kanzleirisikoanalyse zu verwenden. Die Höhe des im Risikoprofil festgestellten auftragsbezogenen Risikos bestimmt auch, ob geringere Sorgfaltspflichten oder erhöhte Sorgfaltspflichten anzuwenden sind. Von dieser Risikoeinstufung hängt z.B. weiters auch die Frequenz der turnusmäßigen Aktualisierung der dokumentierten Daten ab. Hierbei gilt, dass Daten zu einem Auftrag mit einem erhöhten Risiko auch ohne Anlass öfters zu aktualisieren sind als zu einem Auftrag mit niedrigerem Risiko. Bei einem Auftrag mit erhöhtem Risiko ist zumindest eine jährliche Aktualisierung des Risikoprofils notwendig.

### **Sorgfaltspflichten beim Kundenannahmeprozess**

Bei einer natürlichen Person als Auftraggeber hat die Identifikation durch einen aktuellen amtlichen Lichtbildausweis zu erfolgen. Dasselbe gilt für die gesetzlichen Vertreter bei nicht natürlichen Personen als Auftraggeber in vertretungsbefugter Anzahl (§ 90 Z 1 WTBG 2017 – Umfang der Sorgfaltspflichten). Ein im Laufe der Geschäftsbeziehung ablaufender Lichtbildausweis ändert nichts an der ursprünglichen Identifikation. Geeignete Lichtbildausweise haben mit einem nicht austauschbaren – d.h. von der Behörde anzubringenden – erkennbaren Kopfbild der zu identifizierenden Person versehen zu sein, das nicht offenkundig von der sich persönlich ausweisenden Person abweicht.

Steht für die Identifikation einer natürlichen Person kein aktueller amtlicher Lichtbildausweis zu Verfügung dann schreibt § 1 Abs. 1 KSW-GWPRL (Ausgestaltung der Sorgfaltspflichten) vor, dass die Überprüfung risikobasiert auch auf anderen Quellen beruhen kann. Dabei gelten Auskünfte und Informationen von verlässlichen Gewährspersonen als glaubwürdig. Zu diesen zählen Gerichte und sonstige staatliche Behörden, Steuerberater, Wirtschaftsprüfer und Personen mit vergleichbarer ausländischer Berufsbefugnis, Notare, Rechtsanwälte und Kreditinstitute, sofern sie nicht ihren amtlichen Wirkungsbereich, Sitz oder Wohnsitz in einem Nicht-Kooperationsstaat im Sinne des § 94 Abs. 5 WTBG (Verstärkte Sorgfaltspflichten) haben.

### **Prüfungen ungewöhnlicher Transaktionen**

Ungewöhnliche Transaktionen iSd § 94 Abs. 1 Z 1 WTBG 2017 führen jedenfalls dazu, dass Berufsberechtigte die Risikoeinstufung – bis zur Klärung – auf hohes Risiko zu setzen haben. Sie werden außerdem daraufhin zu untersuchen, ob Mittelherkunft und -verwendung legal ist. Dies hat mit angemessenen Mitteln zu erfolgen. Eine ungeklärte Faktenlage könnte den Berufsberechtigten einerseits der Gefahr aussetzen, zum Beitragstäter einer strafrechtlichen Geldwäscherei iSd § 165 StGB zu werden, und andererseits der Pflicht, eine Verdachtsmeldung auf Vorliegen von Finanzmitteln aus kriminellen Handlungen gem. § 96 WTBG 2017 abzugeben, nicht nachzukommen.

### **Verdachtsfälle**

Für die Meldepflicht eines Steuerberaters oder Wirtschaftsprüfers reicht es aus, dass ein Verdacht besteht, dass finanzielle Mittel iSd § 87 Abs. 2 Z 6 WTBG 2017 unabhängig vom jeweiligen Betrag aus krimineller Tätigkeiten iSd § 87 Abs. 2 Z 2 WTBG 2017 stammen oder mit Terrorismusfinanzierung in Verbindung stehen. Berufsberechtigte müssen bei Verdachtsmomenten eine nähere Prüfung der vorliegenden Anhaltspunkte durchführen. § 87 Abs. 2 Z 7 WTBG 2017 definiert einen begründeten Verdacht als "die Annahme der

Wahrscheinlichkeit des Vorliegens eines bestimmten Sachverhalts, die sich aufgrund der Kenntnis hinreichender tatsächlicher Anhaltspunkte ergibt. Diese Annahme hat über eine bloße Vermutung hinauszugehen.“ Danach besteht ein Verdacht dann, wenn "hinreichende tatsächliche Anhaltspunkte die Annahme der Wahrscheinlichkeit des Vorliegens bestimmter Umstände rechtfertigen, wobei ein Verdacht mehr als eine bloße Vermutung ist. Ein Verdacht kann immer nur auf Grund von Schlussfolgerungen aus Tatsachen entstehen – aus der Kenntnis von Tatsachen kann nach der Lebenserfahrung auf ein Vergehen geschlossen werden." Abschließend ist noch anzumerken, dass soweit davon ausgegangen wird, die Anforderungen an einen „berechtigten Grund zur Annahme“ seien geringer als die an den Verdacht, sind Zweifel angezeigt, weil kaum erkennbar ist, inwiefern der Verdacht – angesichts der dargestellten Definition – höhere Anforderungen stellt als das Vorliegen berechtigter Gründe zur Annahme eines Kontakts mit inkriminiertem Vermögen. (Brandl/Bülte, Die Geldwäsche-Verdachtsmeldepflicht und das Vertrauensverhältnis zwischen Berater und Mandant in Leitner/Brandl (Hrsg), Finanzstrafrecht 2019)

### **Meldepflicht**

Ergibt sich für den Berufsberechtigten bei der Ausübung seiner beruflichen Tätigkeit ein Verdacht, dass finanzielle Mittel unabhängig vom jeweiligen Betrag aus kriminellen Tätigkeiten stammen oder mit Terrorismusfinanzierung in Verbindung stehen, hat er die Geldwäschemeldestelle von sich aus mittels einer Meldung unverzüglich zu informieren (§ 96 Abs. 1 WTBG 2017). Ferner hat er eine Verdachtsmeldung in Erwägung zu ziehen, wenn er bei einem Auftraggeber seinen Sorgfaltspflichten in Bezug auf die Feststellung und Überprüfung der Identität des Auftraggebers, des wirtschaftlichen Eigentümers oder der Bewertung und angemessene Informationseinholung über Zweck und angestrebte Art der Geschäftsbeziehung nicht nachkommen kann (§ 96 Abs. 3 WTBG 2017).

Zusätzlich hat er gemäß § 96 Abs. 2 WTBG 2017 der Geldwäschemeldestelle auf schriftliches Verlangen unmittelbar oder mittelbar alle zusätzlichen Informationen unverzüglich zur Verfügung zu stellen, soweit dem nicht verfahrens- oder berufsrechtliche Verbote oder Aussageverweigerungsrechte entgegenstehen. Die Meldepflicht sowie generell die Anwendung der Regelungen betreffend Geldwäscheprävention in den §§ 88 – 100 WTBG 2017 ist so zu verstehen, dass sich diese ausschließlich auf bei Ausübung der beruflichen Tätigkeit der Berufsberechtigten aufgetretene Tatsachen bezieht.

### **Risikominimierende Maßnahmen der KSW**

Zusätzlich zu den folgenden risikominimierenden Maßnahmen, verweisen wir noch auf die Ausführungen unter den Punkt „(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance“, welche auch als risikominimierende Maßnahmen der KSW zu qualifizieren sind.

### **Schulungen in Bereich Geldwäscheprävention und Terrorfinanzierung durch die KSW**

Die KSW ist stets bedacht ihre Mitglieder im Bereich Geldwäsche und Terrorfinanzierung zu schulen und informiert zu halten. Dies erfüllt die KSW einerseits selbst durch die Organisation von Informationsveranstaltungen und Themenabenden sowie durch den Versand von Newslettern. Zusätzlich können sich Berufsberechtigte auch schriftlich und telefonisch bei der KSW in Hinblick auf Verhinderung von Geldwäsche und Terrorfinanzierung beauskunften lassen. Außerdem sind Steuerberater und Wirtschaftsprüfer gesetzlich verpflichtet ein vorgegebenes Maß an Weiterbildungen nachzuweisen. Diese Weiterbildungen werden größtenteils bei der Akademie der Steuerberater und Wirtschaftsprüfer (ASW), einer 100% Tochter der KSW, absolviert. Die ASW hat in den letzten Jahren ihr Angebot an Lehr- und Weiterbildungskursen mit dem

Fokus auf Verhinderung von Geldwäsche und Terrorfinanzierung stark erweitert. Die ASW fungiert des Weiteren als die Ausbildungsakademie für Berufsanwärter/innen. Auch Berufsanwärter/innen werden daher verstärkt im Rahmen ihrer berufsrechtlichen Ausbildung zum Thema Verhinderung von Geldwäsche und Terrorfinanzierung geschult. An dieser Stelle ist weiters die Geldwäschepräventions-Schulungs-App der ASW zu erwähnen. Diese Schulungs-App wird von vielen Berufsberechtigten zur Weiterbildung und zur Schulung von Kanzleimitarbeitern genutzt und hilft sowohl den Berufsstand als auch deren Mitarbeiter zu sensibilisieren.

#### **Das Hinweisgebersystem der KSW gem. § 100 WTBG 2017**

Seit 1. Jänner 2019 verfügt die KSW über ein Hinweisgebersystem. Dieses Hinweisgebersystem ist jedermann zugänglich und dient der anonymen Anzeige von Berufsberechtigten, welche sich nicht an die laut dem WTBG 2017 vorgegeben Maßnahmen zur Verhinderung der Geldwäsche und Terrorismusfinanzierung halten. Jede Anzeige eines Hinweisgebers wird durch die KSW geprüft und kann gegebenenfalls zur Einleitung einer anlassbezogenen Prüfung sowie der Einleitung eines Disziplinarverfahrens führen.

Bis Mai 2020 kam es nur zu einer Meldung über das Hinweisgebersystem der KSW. Diese Meldung betraf jedoch die vermeintliche Geldwäschetätigkeit eines Klienten eines Berufsberechtigten, weshalb sie an die Geldwäschemeldestelle (A-FIU), weitergeleitet wurde.

#### **Gesamtrisiko**

Das Gesamtrisiko der Sektoren Steuerberatung und Wirtschaftsprüfung wird mit gering bis mittel eingestuft.

#### **Empfehlungen**

Zur Verbesserung der Prävention von Geldwäscherei und Terrorismusfinanzierung würde die KSW einen besseren und umfangreicheren Informationsaustausch unter den Behörden anregen. So sollte es eine aktive Informationsweiterleitung der Geldwäschemeldestelle an die KSW geben, wenn Berufsberechtigte betroffen sind oder Vorgänge entdeckt werden, welche eine Erhöhung des Missbrauchs der Dienstleistungen von Steuerberater und Wirtschaftsprüfer indizieren. Des Weiteren sollte auch der Informationsaustausch mit anderen Behörden und Institutionen, wie etwa mit der FMA, der OeNB oder den Finanzinstituten verstärkt und weiter forciert werden.

# Sektorrisikoanalyse Bilanzbuchhaltung

Dienste der Bilanzbuchhalter, Buchhalter und Personalverrechner
<b>Allgemeine Informationen</b>
<p>Mit Inkrafttreten des Bundesgesetzes über die Bilanzbuchhaltungsberufe (Bilanzbuchhaltungsgesetz 2014 - <b>BiBuG 2014</b>, BGBl. I Nr. 191/2013) ist der <b>Präsident der Wirtschaftskammer Österreich</b> seit 1.1.2014 als <b>Bilanzbuchhaltungsbehörde</b>, d.h. als <b>Bundesbehörde im vom BMDW übertragenen Wirkungsbereich, zuständig für die Bilanzbuchhaltungsberufe</b>.</p> <p>Die <b>Geschäftsstelle der Bilanzbuchhaltungsbehörde</b> in der Wirtschaftskammer Österreich übernimmt die <b>operative Ausübung</b> dieser Zuständigkeit.</p> <p>Bilanzbuchhaltungsberufe sind gemäß § 1 BiBuG 2014 die Berufe <b>Bilanzbuchhalter, Buchhalter und Personalverrechner</b>.</p> <p>Gemäß § 6 BiBuG 2014 können nur <b>natürliche Personen, die öffentlich bestellt</b> wurden, und <b>Gesellschaften, die anerkannt</b> wurden, die Befugnisse im Rahmen des jeweiligen Berechtigungsumfangs gemäß §§ 2 - 5 BiBuG 2014 ausüben.</p> <p>Berufsberechtigte der Bilanzbuchhaltungsberufe sind verpflichtet die <b>Maßnahmen zur Verhinderung der Geldwäsche und der Terrorismusfinanzierung gemäß §§ 43 - 52d BiBuG 2014</b> umzusetzen.</p> <p>Dem Präsidenten der WKÖ obliegt gemäß § 52f BiBuG 2014 die <b>Aufsicht über deren Einhaltung</b>.</p>
<b>Bedrohung</b>
<p><b>Terrorismusfinanzierung:</b></p> <p>In den zusammengefassten Szenarien der SNRA wurde die <b>Bedrohung</b>, dass <b>Berufsberechtigte der Bilanzbuchhaltungsberufe</b> für terroristische Aktivitäten missbraucht werden, <b>mit einem hohen Risiko</b> eingestuft. In der Folge soll die <b>nationale Bedrohung</b> abgeleitet werden.</p> <p>Das Bild des Sektors der Bilanzbuchhaltungsberufe ist aus Sicht der Terrorismusfinanzierung <b>völlig eindeutig</b>: die <b>Berufsberechtigten</b> der Bilanzbuchhaltungsberufe kommen <b>mit Bedrohungen in Zusammenhang mit TF nicht in Kontakt</b>.</p> <p>Dieses Bild ergibt sich sehr klar <b>aus den aktuellen Informationen (Befragung von 4.213 Berufsberechtigten, Stand 31.7.2020)</b>, die der Bilanzbuchhaltungsbehörde auf Grundlage der Durchführung ihrer Aufsichtspflichten gemäß § 52f BiBuG 2014 vorliegen. Dies ist wohl primär auf die <b>typische Auftraggeberstruktur</b> und die <b>typischerweise erbrachten Dienstleistungen</b> der Bilanzbuchhaltungsberufe zurückzuführen.</p> <p>So haben die durchschnittlichen Berufsberechtigten der Bilanzbuchhaltungsberufe aus Sicht der Terrorismusfinanzierung <b>keine auffälligen Auftraggeber</b> und <b>kennen</b> deren <b>Geschäftsgewerung vollständig</b>. Dies hängt u.a. damit zusammen, dass Berufsberechtigte ihre Auftraggeber <b>fast ausschließlich in ihrem lokalen Umfeld haben und seit längerer Zeit kennen</b>.</p>

Bestätigt werden diese Informationen ferner durch das **bisherige Ausbleiben (Stand 25.2.2021)** einer Meldung über das **internetbasierte Hinweisgebersystem der Bilanzbuchhaltungsbehörde** gemäß § 52e BiBuG 2014.

Seitens des BMDW und der Geldwäschemeldestelle im Rahmen der Verpflichtung gemäß **§ 52i Abs. 2 BiBuG 2014** wurden der Bilanzbuchhaltungsbehörde Informationen im Rahmen eines informellen Gespräches zur Verfügung gestellt.

**Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine hohe Bedrohung nahelegen, zeigen die aktuellen nationalen Daten aus den oben angeführten Gründen das Gegenteil. Zusammenfassend ist die Bedrohung mit einem niedrigem Risiko für die Bilanzbuchhaltungsberufe einzustufen.**

**Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die **Bedrohung, dass Berufsberechtigte der Bilanzbuchhaltungsberufe für Geldwäscherei missbraucht werden, mit einem hohen Risiko** eingestuft. In der Folge soll die **nationale Bedrohung** abgeleitet werden.

Das Bild des Sektors der Bilanzbuchhaltungsberufe ist aus Sicht der Geldwäscherei auch **sehr klar**: die **durchschnittlichen Berufsberechtigten** der Bilanzbuchhaltungsberufe kommen **mit einer Bedrohung in Zusammenhang mit GW nur selten in Kontakt**.

Dieses Bild ergibt sich ebenso sehr klar **aus den aktuellen Informationen (Befragung von 4213 Berufsberechtigten, Stand 31.7.2020)**, die der Bilanzbuchhaltungsbehörde auf Grundlage der Durchführung ihrer Aufsichtspflichten gemäß § 52f BiBuG 2014 vorliegen. Dieses Bild **trifft** außerdem – mit sehr geringen Schwankungen – **auch auf die einzelnen Bundesländer zu**.

Durch die **tendenziell kleinen Geschäftsstrukturen** (durchschnittlich 1,4 Angestellte) der Berufsberechtigten scheint eine **grundsätzliche Abneigung** zu bestehen, **einzelne Auftraggeber mit potentiell hohem GW-Risiko anzunehmen**, bzw. **große Vorsicht bei der Annahme** zu herrschen, in Befürchtung von Verwaltungsaufwand und/oder Sanktionen/Konsequenzen, die mit solchen Auftraggebern einhergehen. Auch die – oben bereits erwähnte – **typische Auftraggeberstruktur**, bestehend aus Auftraggebern, die **fast ausschließlich aus dem lokalen Umfeld stammen und seit längerer Zeit gekannt werden** ist in diesem Zusammenhang zu nennen.

Die **geographische Natur der Auftraggeberstruktur der Bilanzbuchhaltungsberufe** geht **eindeutig** aus den aktuellen Informationen (Stand 31.7.2020) hervor, die der Bilanzbuchhaltungsbehörde auf Grundlage der Durchführung ihrer Aufsichtspflichten gemäß § 52f BiBuG 2014 vorliegen. Die Auftraggeber der Bilanzbuchhaltungsberufe sind:

- zu **97,79% österreichische Auftraggeber** mit ausschließlichem Hauptwohnsitz dort
- zu **2,08% Auftraggeber aus der EU**
  - mit klarem Bezug zum CEE-Raum bzw. den benachbarten Mitgliedstaaten
  - mit dem stärksten Bezug zu Deutschland
- zu **99,87% Auftraggeber aus Niedrigrisikoländern**
- zu **0,13% Auftraggeber aus Hochrisikoländern**
  - mit klarem Bezug zum CEE-Raum: insbesondere Serbien, Bosnien und die Türkei
  - mit doch relevantem Bezug zu China und Russland



Bestätigt werden diese Informationen wiederum durch das **bisherige Ausbleiben (Stand 25.2.2021)** einer Meldung über das **internetbasierte Hinweisgebersystem der Bilanzbuchhaltungsbehörde** gemäß § 52e BiBuG 2014.

Seitens des BMDW und Geldwäschemeldestelle im Rahmen der Verpflichtung gemäß **§ 52i Abs. 2 BiBuG 2014** wurden der Bilanzbuchhaltungsbehörde Informationen im Rahmen eines informellen Gespräches zur Verfügung gestellt.

#### **Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine hohe Bedrohung nahelegen, zeigen die aktuellen nationalen Daten aus den oben genannten Gründen das Gegenteil. Zusammenfassend ist die Bedrohung mit einem niedrigen Risiko für die Bilanzbuchhaltungsberufe einzustufen.**

#### **Verletzbarkeit**

##### **Terrorismusfinanzierung:**

In den zusammengefassten Szenarien der SNRA wurde die **Verletzbarkeit von Berufsberechtigten der Bilanzbuchhaltungsberufe** im Hinblick auf den Missbrauch für die Zwecke der Terrorismusfinanzierung mit einem hohen Risiko eingestuft. In der Folge soll die **nationale Verletzbarkeit** abgeleitet werden.

##### **(a) Risikopotential:**

Wie oben beschrieben, ist das Bild des Sektors der Bilanzbuchhaltungsberufe aus Sicht der Terrorismusfinanzierung **völlig eindeutig**: die **Berufsberechtigten** der Bilanzbuchhaltungsberufe kommen **mit Bedrohungen in Zusammenhang mit TF nicht in Kontakt**.

Der Sektor der Bilanzbuchhaltungsberufe scheint **aufgrund der von den Berufsberechtigten typischerweise erbrachten Dienstleistungen** grundsätzlich **nicht für TF attraktiv** zu sein.

##### **(b) Risikobewusstsein:**

Es besteht ein **hohes Risikobewusstsein** bei allen Berufsberechtigten der Bilanzbuchhaltungsberufe.

##### **(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Berufsberechtigte der Bilanzbuchhaltungsberufe sind **verpflichtet** die **Maßnahmen zur Verhinderung der Geldwäsche und der Terrorismusfinanzierung gemäß §§ 43-52d BiBuG 2014** umzusetzen und ihre diesbezüglichen **Verpflichtungen einzuhalten**.

**Verstöße** gegen die berufsrechtlichen **Verpflichtungen iZm der GW/TF – Prävention werden gem. §§ 52j - 52k BiBuG unter Strafe gestellt**.

Die Bilanzbuchhaltungsbehörde, der die Aufsicht der Einhaltung der Vorkehrungen iZm der GW/TF-Prävention obliegt, hat für die im letzten Jahr durchgeführte Befragung der Berufsberechtigten eine **standardisierte Risikoanalyse** (samt Erklärungen und Begriffsbestimmungen) erstellt (siehe Homepage der Bilanzbuchhaltungsbehörde unter <https://www.wko.at/site/bilanzbuchhaltung/verhinderung-geldwaesche-terrorismusfinanzierung.html>). Diese Risikoanalyse soll die Berufsberechtigten bei der Erfüllung ihrer berufsrechtlichen Verpflichtungen iZm GW/TF-Prävention unterstützen und kann seitens der Behörde auch als **Grundlage für eine anlassbezogene bzw auch anlassunabhängige Prüfung** gem. §§ 52g ff BiBuG herangezogen werden.

##### **Human- und Finanzressourcen:**

Der Bilanzbuchhaltungsbehörde steht eine **Teilzeitkraft zur Verfügung** für die Betreuung des Bereiches GW/TF-Prävention.

**Conclusio:**

Ausgehend von den zusammengefassten Szenarien der SNRA, die eine hohe Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von Bilanzbuchhaltungsberufe, für die Zwecke der Terrorismusfinanzierung missbraucht zu werden, mit einem niedrigem Risiko einzustufen ist.

**Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von **Berufsberechtigten der Bilanzbuchhaltungsberufe** im Hinblick auf den Missbrauch für die Zwecke der Geldwäscherei **mit einem hohen Risiko** eingestuft. In der Folge soll die **nationale Verletzbarkeit** abgeleitet werden.

**(a) Risikopotential:**

Wie oben beschrieben, ist das Bild des Sektors der Bilanzbuchhaltungsberufe aus Sicht der Geldwäscherei **sehr klar**: die **durchschnittlichen Berufsberechtigten** der Bilanzbuchhaltungsberufe kommen **mit einer Bedrohung in Zusammenhang mit GW nur selten in Kontakt**.

Anfälligkeit/Verletzbarkeit **aus geographischer Sicht** besteht in **verschwindend geringem Ausmaß**: Dadurch, dass die typische Auftraggeberstruktur fast ausschließlich aus österreichischen bzw. geographischen Niedrigrisikoauftraggebern aus dem näherem Umfeld besteht, besteht nämlich eine **erhöhte Sensibilität gegenüber Auftraggebern, die nicht in dieses typische Schema fallen**.

Anfälligkeit/Verletzbarkeit **aus Sicht der Tätigkeiten der von den Auftraggebern angebotenen Produkte, Dienstleistungen, Transaktionen und/oder Vertriebskanäle** besteht ebenso in **verschwindend geringem Ausmaß**.

Anfälligkeit/Verletzbarkeit **aus Sicht der Tätigkeiten der Auftraggeber** besteht hingegen in **einem geringen, aber doch relevantem Ausmaß** hinsichtlich der **bargeldintensiven Abwicklung** der Tätigkeiten der Auftraggeber. Dieser Aspekt ist mitunter auf die **Auftraggeberstruktur** der Bilanzbuchhaltungsberufe **zurückzuführen**, die zu einem großen Teil aus Gastronomie, Handel und Handwerk ausgemacht wird.

Dieses Bild **trifft** außerdem – mit sehr geringen Schwankungen – **auch auf die einzelnen Bundesländer zu**. Conclusio: Niedriges Risiko, aus den angeführten Gründen.

**(b) Risikobewusstsein:**

Es besteht ein **hohes Risikobewusstsein** bei allen Berufsberechtigten der Bilanzbuchhaltungsberufe.

**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Berufsberechtigte der Bilanzbuchhaltungsberufe sind **verpflichtet** die **Maßnahmen zur Verhinderung der Geldwäsche und der Terrorismusfinanzierung gemäß §§ 43 - 52d BiBuG 2014 umzusetzen** und ihre diesbezüglichen **Verpflichtungen einzuhalten**.

**Verstöße** gegen die berufsrechtlichen **Verpflichtungen iZm der GW/TF – Prävention werden gem. §§ 52j - 52k BiBuG unter Strafe gestellt**.

Die Bilanzbuchhaltungsbehörde, der die Aufsicht der Einhaltung der Vorkehrungen iZm der GW/TF-Prävention obliegt, hat für die im letzten Jahr durchgeführte Befragung der Berufsberechtigten eine **standardisierte Risikoanalyse** (samt Erklärungen und Begriffsbestimmungen) erstellt (siehe Homepage der Bilanzbuchhaltungsbehörde unter

<https://www.wko.at/site/bilanzbuchhaltung/verhinderung-geldwaesche-terrorismusfinanzierung.html>). Diese Risikoanalyse soll die Berufsberechtigten bei der Erfüllung ihrer beruflichen Verpflichtungen iZm GW/TF-Prävention unterstützen und kann seitens der Behörde auch als **Grundlage für eine anlassbezogene bzw auch anlassunabhängige Prüfung** gem. §§ 52g ff BiBuG herangezogen werden.

**Human- und Finanzressourcen:**

Der Bilanzbuchhaltungsbehörde steht eine **Teilzeitkraft zur Verfügung** für die Betreuung des Bereiches GW/TF-Prävention.

**Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine hohe Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von Berufsberechtigten der Bilanzbuchhaltungsberufe, für die Zwecke der Geldwäscherei missbraucht zu werden, mit einem niedrigem Risiko einzustufen ist.**

**Risikomindernde Maßnahmen**

- Fortlaufende Sensibilisierung im Rahmen der Fortbildungspflicht gemäß § 33 Abs. 3 BiBuG 2014
- Sensibilisierung im Rahmen der Durchführung der Aufsichtspflichten gemäß § 52f BiBuG 2014 durch die Bilanzbuchhaltungsbehörde, etwa durch die Zurverfügungstellung von Fallbeispielen und Orientierungshilfen auf ihrer Website (<https://www.wko.at/site/bilanzbuchhaltung/verhinderung-geldwaesche-terrorismusfinanzierung.html>)

**Gesamtrisiko**

**Zusammenfassend ist das Risiko als gering einzustufen.**

# Sektorrisikoanalyse Glücksspiel

<b>Ausspielungen in Spielbanken (Casinos)</b>
<b>Allgemeine Informationen</b>
Ausspielungen in Spielbanken sind Glücksspieldienste iS der Richtlinie (EU) 2015/849 (Art. 3 Z 14), die in der Form von terrestrischem Glücksspiel (an einem physischen Ort, automatisiert oder in der Form von Lebendspiel) angeboten werden. Derzeit werden im Bundesgebiet 12 Spielbanken von einem einzigen Anbieter betrieben.
<b>Bedrohung</b>
<b>Terrorismusfinanzierung:</b> In den zusammengefassten Szenarien der SNRA wurde die Bedrohung, dass Spielbanken für terroristische Aktivitäten missbraucht werden, mit einem nicht relevanten Risiko eingestuft. Auch die nationale Bedrohung wird als nicht relevant eingestuft.
<b>Conclusio:</b> <b>Zusammenfassend ist die Bedrohung mit nicht relevant einzustufen.</b>
<b>Geldwäscherei:</b> In den zusammengefassten Szenarien der SNRA wurde die Bedrohung mit einem <b>sehr hohen</b> Risiko eingestuft. In der Folge soll die nationale Bedrohung abgeleitet werden: Bedrohungen bestehen durch unbekannte Kundenherkunft, Mehrfachregistrierungen einer Person, Nutzung von Bargeld, Nutzung von Fremdwährungen, Mehrfachnutzung von Zahlungsmethoden durch mehrere Kunden, Spielteilnahme von politisch exponierten Personen (PEP), Spielteilnahme auf Sanktionslisten gelisteter Personen, Missbrauch von Depots, Umgehung der Einzahlungslimits, Malversationen eines Mitarbeiters (Ausstellung von Gewinnbestätigungen/Zusammenarbeit Gast und Dealer), Umwandlung von Bargeld, Falschgeld, Zusammenspiel von Kunden/Gästen, Nichtweiterbehandlung eines Geldwäschereiverdachts. Insgesamt ist das Risiko dieser Bedrohungen mit <b>hoch</b> einzustufen.
<b>Conclusio:</b> <b>Ausgehend von den zusammengefassten Szenarien der SNRA, die ein sehr hohes Risiko der Bedrohung nahelegen, zeigen die aktuellen nationalen Daten ein hohes Risiko. Zusammenfassend ist die Bedrohung mit hoch einzustufen.</b>
<b>Verletzbarkeit</b>
<b>Terrorismusfinanzierung:</b> In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von Spielbanken im Hinblick auf den Missbrauch für die Zwecke der Terrorismusfinanzierung als <b>nicht relevant</b> eingestuft. Die nationale Verletzbarkeit wird ebenfalls als <b>nicht relevant</b> bewertet.
<b>Conclusio:</b> <b>Zusammengefasst ist die Verletzbarkeit von Spielbanken für die Zwecke der Terrorismusfinanzierung missbraucht zu werden, mit nicht relevant einzustufen.</b>
<b>Geldwäscherei:</b> In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von Spielbanken im Hinblick auf den Missbrauch für die Zwecke der Geldwäscherei als <b>mittel</b> eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden:

**(a) Risikopotential:**

Es besteht ein sehr hoher Anteil an Barumsätzen und die Möglichkeit der Umwandlung von Bargeld in Spielgeld und vice versa.

**(b) Risikobewusstsein:**

Nicht zuletzt aufgrund der Vorgaben der EU-Geldwäscherichtlinie wurden verstärkte Sorgfaltspflichten in die nationale Glücksspielgesetzgebung aufgenommen. Der Zutritt zu Spielbanken wird erst nach Vorlage eines amtlichen Lichtbildausweises gestattet. Eine Spielteilnahme ist überwiegend nur mit personifizierter Spielerkarte möglich. Zudem wird dem Risiko der Geldwäscherei durch entsprechende Überwachungssysteme in den Spielbanken und durch regelmäßige Teilnahme der Mitarbeiter an Geldwäscherei-Präventionsschulungen entgegengetreten.

**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

§ 31c GSpG iVm FM-GwG sieht umfassende Sorgfaltspflichten für die Betreiber von Spielbanken vor (entsprechend der jeweiligen Sachlage neben der Feststellung der Identität der Besucher insb. die Feststellung der Mittelherkunft oder des wirtschaftlichen Eigentümers).

**Conclusio:**

**Ausgehend von der SNRA, die eine mittlere Verletzbarkeit nahelegt, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von Spielbanken, für Zwecke der Geldwäscherei missbraucht zu werden, mit mittel einzustufen ist.**

**Risikomindernde Maßnahmen**

Umfassende Sorgfaltspflichten in Bezug auf die Prävention von Geldwäscherei sind gem. § 31c GSpG iVm FM-GwG neben der Verpflichtung zur Erstellung einer Risikoanalyse und der lückenlosen Identitätsfeststellung der Besucher, je nach Sachlage die Feststellung der Identität eines Treugebers/wirtschaftlichen Eigentümers, der Mittelherkunft und die Überprüfung des Zwecks/Art der Geschäftsbeziehung sowie deren kontinuierliche Überwachung als auch die Bereithaltung der vom Glücksspielgesetz geforderten Dokumentation. Das Glücksspielgesetz verpflichtet den Bundesminister für Finanzen gegenüber den Spielbankbetreibern zur Zurverfügungstellung von aktuellen Informationen über Methoden der bzw. Anhaltspunkte für Geldwäscherei und Terrorismusfinanzierung. Der Bundesminister für Finanzen hat außerdem für eine zeitgerechte Rückmeldung in Bezug auf Verdachtsmeldungen bei Geldwäscherei oder Terrorismusfinanzierung und die daraufhin getroffenen Maßnahmen zu sorgen und ein Hinweisgebersystem für die Meldung von Verstößen gegen die Geldwäschereibestimmungen einzurichten.

**Gesamtrisiko**

Zusammenfassend ist das Risiko als **mittel** einzustufen.

**Empfehlungen**

Weitere Intensivierung der Zusammenarbeit zwischen Unternehmen und Behörden und möglichst zeitnahe Auskunft bei Geldwäschereiverdachtsmomenten.

## Klassische Lotterien, sonstige elektronische Lotterien, elektronische Lotterien über Video-Lotterie-Terminals

### Allgemeine Informationen

Lotterien sind Glücksspieldienste iSd Art. 3 Z 14 der Richtlinie (EU) 2015/849. Lotterien werden als **klassische Lotterien, elektronische Lotterien über Video-Lotterie-Terminals** (Zugang über zentralseitig vernetzte Terminals an ortsfesten, öffentlich zugänglichen Betriebsstätten) und **sonstige elektronische Lotterien** (Spilteilnahme unmittelbar durch den Spieler über elektronische Medien und zentralseitig herbeigeführte Entscheidung über das Spielergebnis, z.B. **Online-Glücksspiel**) zur Verfügung gestellt. Derzeit werden alle Formen von Lotterien von einem einzigen Anbieter betrieben.

### Bedrohung

#### Terrorismusfinanzierung:

Sowohl die SNRA als auch die nationale Risikoanalyse gelangen zu dem Ergebnis, dass das Risiko, dass Lotterien für terroristische Aktivitäten missbraucht werden, als **nicht relevanten** einzustufen ist.

#### Conclusio:

**Zusammenfassend ist die Bedrohung mit nicht relevant einzustufen.**

#### Geldwäscherei:

In den zusammengefassten Szenarien der SNRA wurde die Bedrohung in Bezug auf **klassische Lotterien** mit einem **mittleren** Risiko, in Bezug auf **elektronische Lotterien über VLT** mit einem **mittleren** Risiko und in Bezug auf **sonstige elektronische Lotterien** mit einem **hohen** Risiko eingestuft. In der Folge soll die nationale Bedrohung abgeleitet werden:

- Hinsichtlich klassischer Lotterien können keine nationalen Bedrohungen identifiziert werden. Der Verkauf klassischer Lotterienprodukte (insb. Lottoschein, Sofortlotterien) erfolgt ausschließlich über die Vertragspartner im Inland und in Euro. Ein allfälliger Gewinn wird im Rahmen einer öffentlichen und notariell beaufsichtigten Ziehung festgestellt bzw. bei Sofortlotterien bereits im Vorhinein festgelegt und schließt somit auch die Möglichkeit von Malversationen durch Mitarbeiter aus. Aufgrund der Anonymität der Gewinner ist auch eine Kontaktierung durch Kriminelle mit der Absicht, ein gewinnendes Ticket für Geldwäscheziele zu erwerben und einzulösen, sehr unwahrscheinlich. Ab einer Gewinnauszahlung von EUR 1.000,10 erfolgt zudem eine Identifizierung des Gewinners. Das nationale Risiko klassischer Lotterien ist somit als niedrig einzustufen.
- Nationale Bedrohungen im Bereich elektronische Lotterien über Video-Lottery-Terminals (VLT): Den Risiken Wegfall einer Face-to-Face Identifizierung, Mehrfachregistrierung einer Person, Mehrfachnutzung von Zahlungsmethoden durch mehrere Kunden, Markiertes Geld und Falschgeld wird insofern begegnet, als sich die Spieler vor Spielteilnahme registrieren und mit einem amtlichen Lichtbildausweis auszuweisen haben. Die Spielteilnahme ist zudem nur mittels personifizierter Spielkarte möglich und eine Mehrfachregistrierung einer Person somit ausgeschlossen. Bei Wechselungen in Spielgeld erfolgt eine Prüfung der Geldscheine durch einen Banknotenakzeptor, um die Zuführung von markiertem Geld oder Falschgeld auszuschließen. Unbare Zahlungen werden ausschließlich über einen Mitarbeiter abgewickelt, welcher die Identität des Kunden überprüft, weshalb es auch nicht möglich ist, dasselbe unbare Zahlungsmittel durch mehrere Kunden zu nutzen. Die nationale Bedrohung ist daher mit einem niedrigen Risiko einzustufen.
- Nationale Bedrohungen im Bereich der sonstigen elektronischen Lotterien sind: Wegfall einer Face-to-Face Identifizierung, Mehrfachregistrierungen einer Person,

Mehrfachnutzung von Zahlungsmethoden durch mehrere Kunden, Missbrauch von Depots, Umgehung der Einzahlungslimits, Spielteilnahme von politisch exponierten Personen (PEP), Spielteilnahme auf Sanktionslisten gelisteter Personen, Zusammenspiel von Kunden bei Poker und die Nichtbehandlung von Geldwäschereiverdachtsmomenten. Auf nationaler Ebene ist daher von einem mittleren Risiko auszugehen.

**Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine mittlere Bedrohung nahelegen, zeigen die aktuellen nationalen Daten insgesamt ein niedriges Risiko. Zusammenfassend ist die Bedrohung als niedrig einzustufen.**

**Verletzbarkeit**

**Terrorismusfinanzierung:**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von Lotterien im Hinblick auf den Missbrauch für die Zwecke der Terrorismusfinanzierung als **nicht relevant** eingestuft. Auch die nationale Verletzbarkeit ist als **nicht relevant** zu bewerten.

**Conclusio:**

**Zusammengefasst ist von einer nicht relevanten Verletzbarkeit auszugehen.**

**Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit im Hinblick auf den Missbrauch für die Zwecke der Geldwäscherei in Bezug auf klassische Lotterien mit **mittel**, in Bezug auf elektronische Lotterien über Video-Lottery-Terminals (VLT) mit **mittel** und in Bezug auf sonstige elektronische Lotterien mit **hoch** eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden:

**(a) Risikopotential:**

Bei **klassischen Lotterien** besteht das Risiko der Geldwäscherei, indem ein Ticket, welches gewonnen hat, dem Gewinner abgeworfen und anschließend eingelöst wird. Hinsichtlich **elektronischer Lotterien über VLT** besteht ein Risiko aufgrund von Barumsätzen bzw. der Ein- und Rückwechslung von Bargeld über Spielerkarten. **Sonstige elektronische Lotterien** bergen das Risiko der Spielteilnahme mittels falscher Identität aufgrund des Wegfalls einer Face-to-Face Identifikation sowie das Risiko der unbekannteren Mittelherkunft aufgrund der Möglichkeit Einsätze mittels Paysafe-Karten und Eurobons zu leisten.

**(b) Risikobewusstsein:**

Dem Risiko des Erwerbs und der Einlösung eines Gewinnertickets bei **klassischen Lotterien** durch Dritte wird durch die Wahrung der Anonymität der Gewinner entgegengetreten. Dadurch ist es nahezu ausgeschlossen, dass Kriminelle mit dem Gewinner in Kontakt treten, um von diesem das gewinnende Ticket zu erwerben und anschließend selbst einzulösen. Zudem ist bei Auszahlungen ab EUR 1.000,10 eine Identifikation zwingend vorgesehen. Bei **elektronischen Lotterien über VLT** gelten Einsatzlimits und verstärkte Sorgfaltspflichten bei Wechselung von Beträgen ab EUR 2.000 in Spielgeld und umgekehrt. Eine Spielteilnahme an elektronischen Lotterien über VLT ist außerdem nur mit personifizierter Spielerkarte nach Vorlage eines amtlichen Lichtbildausweises möglich. Hinsichtlich **sonstiger elektronischer Lotterien** werden erhöhte Anforderungen an die Registrierung gestellt: Eine Spielteilnahme ist erst nach Erfassung der persönlichen Daten möglich. Die Daten werden über Deltavista verifiziert und erfolgt zudem eine Überprüfung der Daten im zentralen Melderegister. Außerdem sind Einsätze mit maximal EUR 800 pro registriertem Spielteilnehmer und Woche für alle Zahlungsarten limitiert. Auszahlungen aus dem elektronischen Spielguthaben erfolgen durch Überweisung auf das vom Spielteilnehmer bekannt gegebene, im EWR-Raum

geführten Bankkonto des Spielteilnehmers. Die Bekanntgabe der Kontoverbindung hat anlässlich der ersten Auszahlungsanforderung zu erfolgen. Hat sich der Spielteilnehmer zu diesem Zeitpunkt noch keiner erweiterten Identifizierung unterzogen, so muss diese unmittelbar vor der ersten Auszahlungsanforderung folgen. Gem. § 6 Abs. 4 FM-GwG werden dafür folgende Identifikationsverfahren angeboten: Onlineverifikation eines amtlichen Lichtbildausweises, Onlineverifikation mittels eID, Onlineverifikation mittels Handysignatur.

**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Die Bestimmungen des Glücksspielgesetzes sehen verstärkte Sorgfaltspflichten zur Verhinderung von Geldwäscherei vor (bspw. für die Aufbuchung von Bargeld auf Spielkarten bei VLT). Außerdem gilt aufgrund der von der Glücksspielaufsicht genehmigten Spielbedingungen für **sonstige elektronische Lotterien** ein Einzahlungslimit von EUR 800 pro registriertem Spielteilnehmer und Woche.

**Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine mittlere Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von Lotterien, für die Zwecke der Geldwäscherei missbraucht zu werden, mit niedrig einzustufen ist.**

**Risikomindernde Maßnahmen**

Für den Lotteriekonzessionär gelten gem. § 31c GSpG iVm FM-GwG umfassende Sorgfaltspflichten in Bezug auf die Prävention von Geldwäscherei. **Klassische Lotterienprodukte** werden ausschließlich im Einzelhandel (Tabak, Trafiken, Tankstellen, Postämter etc.) vertrieben und beläuft sich der durchschnittliche Spieleinsatz dabei auf EUR 5,50. Einzahlungen für **sonstige elektronische Lotterien** sind mit EUR 800 pro registriertem Spielteilnehmer und Woche limitiert. Für die Definition und Umsetzung frühzeitiger Maßnahmen wurde beim Lotteriekonzessionär ein weisungsfreier Geldwäschebeauftragter bestellt und wird außerdem ein zertifiziertes Risikomanagement und –monitoring für auffälliges Spielverhalten betrieben. Zur Vorbeugung von Geldwäscherei erfolgen regelmäßige Schulungen der (Vertriebs-)Mitarbeiter. Gewinne ab EUR 1.000,10 werden nach den von der Glücksspielaufsicht genehmigten Spielbedingungen ausschließlich bei gesondert bezeichneten Großgewinn-Auszahlungsstellen nach Vorlage eines amtlichen Lichtbildausweises ausbezahlt und erfolgt ein periodischer Abgleich der Gewinner mit der PEP-Datenbank. Auszahlungen **sonstiger elektronischer Lotterien** erfolgen ausnahmslos auf EWR-Bankkonten.

**Gesamtrisiko**

Das Gesamtrisiko ist als **niedrig** einzustufen.

**Empfehlungen**

Weitere Intensivierung der Zusammenarbeit zwischen Unternehmen und Behörden und möglichst zeitnahe Auskunft bei Geldwäschereiverdachtsmomenten.



## Landesausspielungen mit Glücksspielautomaten

### Allgemeine Informationen

Landesausspielungen mit Glücksspielautomaten sind Glücksspieldienste iSd Art. 3 Z 14 der Richtlinie (EU) 2015/849 in der Form von terrestrischem Glücksspiel, das an einem physischen Ort ausschließlich mit Glücksspielautomaten (offline) durchgeführt wird. Landesausspielungen mit Glücksspielautomaten sind Ausspielungen mit - einem Typenprüfungsverfahren unterzogenen und elektronisch an ein zentrales Kontrollsystem der obersten Glücksspielbehörde angebotenen – Glücksspielautomaten, bei denen die Entscheidung über das Spielergebnis durch eine mechanische oder elektronische Vorrichtung im Gerät selbst erfolgt, mit limitiertem Einsatz (max. EUR 10) und Gewinn (max. EUR 10.000; keine Jackpots) an ortsfesten, öffentlich zugänglichen Betriebsstätten (Automatensalons mit mindestens 10 und höchstens 50 Glücksspielautomaten oder höchstens drei Glücksspielautomaten in Einzelaufstellung), in denen keine anderen Glücksspiele angeboten werden dürfen (kein Leberndspiel), die zur Einhaltung der an sie gestellten ordnungspolitischen Anforderungen behördlicher Aufsicht unterliegen, mit besonderen Begleitmaßnahmen zur Vorbeugung von Spielsucht sowie Geldwäscherei und Terrorismusfinanzierung.

### Bedrohung

#### **Terrorismusfinanzierung:**

In den zusammengefassten Szenarien der SNRA wurde die Bedrohung, dass Automaten-glücksspiel für terroristische Aktivitäten missbraucht werden, mit einem **nicht relevanten** Risiko eingestuft. In der Folge soll die nationale Bedrohung abgeleitet werden:

Es besteht insofern keine reelle Möglichkeit zur Terrorismusfinanzierung, da keine Online-Teilnahme oder Einsatzleistung bzw. Gewinnauszahlung über elektronischen Zahlungsverkehr möglich ist. Verschleierte Zuwendungen an Terroristen finden daher nicht statt. Im Vorhinein festgelegte Gewinnausschüttungsquoten verhindern eine Vermehrung der eingesetzten Mittel iS einer Finanzierung.

#### **Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine nicht relevante Bedrohung nahelegen, zeigen die aktuellen nationalen Daten, dass eine Finanzierung terroristischer Aktivitäten durch Landesausspielungen mit Glücksspielautomaten als nicht realistisch erscheint und ist ein etwa bestehendes Restrisiko nicht relevant. Zusammenfassend ist die Bedrohung mit nicht relevant einzustufen.**

#### **Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Bedrohung mit einem **mittleren** Risiko eingestuft. In der Folge soll die nationale Bedrohung abgeleitet werden: Automaten-glücksspiel birgt aufgrund der **geringen Beträge**, die bei dieser Form des Automaten-glücksspiels eingesetzt (maximal EUR 10 pro Spiel) und gewonnen werden können (maximal EUR 10.000 pro Spiel, keine Jackpots), ein **geringes** Geldwäscherei-Risiko. Zudem werden alle durchgeführten Spiele (sowie jeder Einsatz und Gewinn) lückenlos elektronisch aufgezeichnet und an das zentrale Kontrollsystem übertragen. Eine Spielteilnahme ist außerdem nur mit **personifizierter Spielkarte** nach Vorlage eines amtlichen Lichtbildausweises möglich.

#### **Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine mittlere Bedrohung nahelegen, zeigen die aktuellen nationalen Daten ein niedriges Risiko.**

## Verletzbarkeit

### **Terrorismusfinanzierung:**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von Automaten-glücksspiel im Hinblick auf den Missbrauch für die Zwecke der Terrorismusfinanzierung als **nicht relevant** eingestuft. Auch die nationale Verletzbarkeit des Automaten-glücksspiels ist als **nicht relevant** einzustufen.

### **Conclusio:**

**Zusammenfassend ist die Verletzbarkeit von Automaten-glücksspiel für Zwecke der Terrorismusfinanzierung als nicht relevant einzustufen.**

### **Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von Automaten-glücksspiel im Hinblick auf den Missbrauch für Zwecke der Geldwäscherei als **mittel** eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden:

#### **(a) Risikopotential:**

Automaten-glücksspiel beruht vorwiegend auf Barumsätzen. Es könnte allenfalls Geldwäscherei betrieben werden, indem ein größerer Barbetrag auf die Spielerkarte aufgebucht wird, um anschließend mit einem geringen Teil dieses Betrages zu spielen und sich den verbleibenden Rest bar auszahlen zu lassen.

#### **(b) Risikobewusstsein:**

Um diesem Risiko zu begegnen, verpflichten Wechselungen von Bargeld in Spielguthaben und umgekehrt ebenso wie – an einem Spieltag oder in mehreren anscheinend zusammenhängenden Vorgängen – kumulierte Einsätze in der Höhe von insgesamt EUR 2.000 oder mehr (bei einem möglichen Höchsteinsatz von EUR 10 pro Spiel) die Anbieter der Landesauspielungen mit Glücksspielautomaten zu verstärkter Sorgfalt (insb. zur Einholung und Überprüfung von Informationen über die Herkunft der eingesetzten Mittel).

#### **(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Das Glücksspielgesetz sieht in Bezug auf Geldwäscherei verstärkte Sorgfaltspflichten für die Aufbuchung von Bargeld auf Spielkarten vor.

### **Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine mittlere Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen und insbesondere die Möglichkeit, nur geringe Beträge einzusetzen dazu, dass die Verletzbarkeit von Automaten-glücksspiel für die Zwecke der Geldwäscherei missbraucht zu werden mit niedrig einzustufen ist.**

## Risikomindernde Maßnahmen

§ 5 Abs. 6 GSpG sieht die sinngemäße Einhaltung der Vorgaben für Spielbanken und Lotterien hinsichtlich Geldwäscherei und Terrorismusfinanzierung für Landesauspielungen mit Glücksspielautomaten vor. Die Identität der Besucher/innen wird gemäß § 31c Abs. 3 Z 1 GSpG anhand eines amtlichen Lichtbildausweises erfasst, der den Anforderungen des § 6 Abs. 2 Z 1 FM-GwG entspricht. Die Daten des amtlichen Lichtbildausweises werden mittels Scans oder durch händische Eingabe festgehalten. Zudem ist eine Spielteilnahme nur mit einer personifizierten Spielerkarte möglich. Insbesondere sind bei Wechselungen von Bargeld

in Spielguthaben oder umgekehrt sowie bei kumulierten Einsätzen ab EUR 2.000 die Einholung und Überprüfung von Informationen über die Herkunft der eingesetzten Mittel vorzunehmen.

#### Gesamtrisiko

Das Gesamtrisiko ist als **niedrig** einzustufen.

#### Empfehlungen

Weitere Intensivierung der Zusammenarbeit zwischen Unternehmen und Behörden und möglichst zeitnahe Auskunft bei Geldwäschereiverdachtsmomenten.

### Wetten

#### Allgemeine Informationen

Wetten sind Glücksspieldienste iSd Art. 3 Z 14 der Richtlinie (EU) 2015/849 und werden aufgrund von Bescheiden, auf Basis der jeweiligen landesgesetzlichen Regelungen über Buchmacher und Totalisateure, angeboten. Die Kompetenz für Gesetzgebung und Vollziehung im Bereich Wetten liegt bei den einzelnen Bundesländern.

#### Bedrohung

##### Terrorismusfinanzierung:

In den zusammengefassten Szenarien der SNRA wurde die Bedrohung, dass Wetten für terroristische Aktivitäten missbraucht werden, mit einem **nicht relevanten** Risiko eingestuft. Auch die nationale Bedrohung wird als **nicht relevant** eingestuft.

##### Conclusio:

**Zusammenfassend ist die Bedrohung mit nicht relevant einzustufen.**

##### Geldwäscherei:

In den zusammengefassten Szenarien der SNRA wurde die Bedrohung mit einem **hohen** Risiko eingestuft. In der Folge soll die nationale Bedrohung abgeleitet werden: Bedrohungen bestehen durch die Infiltration des Geschäftsbereiches durch kriminelle Vereinigungen, Spielmanipulation/Wettbetrug, Kauf eines Gewinntickets, kalkuliertes Wettverhalten und Anonyme Wettabgabe bzw. Kunden ohne Identifizierung. Insgesamt ist von einem **mittleren** Risiko auszugehen.

##### Conclusio:

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine hohe Bedrohung nahelegen, zeigen die nationalen Daten ein mittleres Risiko. Zusammenfassend ist die Bedrohung mit mittel einzustufen.**

#### Verletzbarkeit

##### Terrorismusfinanzierung:

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von Wetten im Hinblick auf den Missbrauch für die Zwecke der Terrorismusfinanzierung mit **nicht relevant** eingestuft. Auch die nationale Verletzbarkeit wird mit **nicht relevant** eingestuft.

##### Conclusio:

**Zusammengefasst ist die Verletzbarkeit von Wetten, für die Zwecke der Terrorismusfinanzierung missbraucht zu werden, mit nicht relevant einzustufen.**

**Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von Wetten im Hinblick auf den Missbrauch für die Zwecke der Geldwäscherei mit **hoch** eingestuft. In der Folge soll die nationale Verletzbarkeit abgeleitet werden.

**(a) Risikopotential:**

Ein Risiko besteht aufgrund des hohen Volumens an Wetteinsätzen, welche zu einem großen Anteil anonym bzw. ohne Identifizierung des Kunden und mittels Bargeldes erfolgen.

**(b) Risikobewusstsein:**

Das Risiko ist den Regulatoren und betroffenen Wettunternehmen bekannt und wird versucht, durch entsprechende Gesetzgebung bzw. unternehmensinterne Maßnahmen entgegenzuwirken.

**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Neben detaillierten landesgesetzlichen Vorgaben zur Bekämpfung von Geldwäscherei gelten in 7 von 9 Bundesländern Einsatzlimits für Wetten, wobei das Einsatzlimit in 5 Bundesländern zwischen EUR 50 und 70 und in zwei weiteren Bundesländern bei EUR 500 bzw. 1.000 liegt. Für die Geldwäscherei von hohen Beträgen wäre somit eine große Anzahl von Wettabgaben an unterschiedlichen Orten erforderlich, was sehr aufwendig wäre und ein hohes Maß an Planung erfordern würde. Um Geldwäscherei zu verhindern, wird zudem durch unternehmensinternes Risiko-Monitoring und Risiko-Management das Wettverhalten der Kunden systematisch überwacht.

**Conclusio:**

**Ausgehend von den zusammengefassten Szenarien der SNRA, die eine hohe Verletzbarkeit nahelegen, führen die dargelegten Rahmenbedingungen dazu, dass die Verletzbarkeit von Wetten, für die Zwecke der Geldwäscherei missbraucht zu werden, mit mittel einzustufen ist.**

**Risikomindernde Maßnahmen**

Die jeweiligen Landesgesetze sehen detaillierte Maßnahmen zur Bekämpfung von Geldwäscherei vor. IT-gestützte Monitoring Systeme dienen der Erkennung von auffälligen Wetten bzw. Transaktionen. Zudem sind die Einsätze im überwiegenden Anteil der Bundesländer limitiert.

**Gesamtrisiko**

Das Gesamtrisiko wird als **mittel** eingestuft.

**Empfehlungen**

Weitere Intensivierung der Zusammenarbeit zwischen Unternehmen und Behörden und möglichst zeitnahe Auskunft bei Geldwäschereiverdachtsmomenten.

## Anhang

### Allgemeine Informationen

<b>Zugewiesene Human- und Finanzressourcen gem. § 3 Abs. 3 Z 7 FM-GwG für den Sektor Glücksspiel</b>		
<b>Gebietskörperschaft</b>	<b>Humanressourcen (VBÄ)*</b>	<b>Finanzressourcen*</b>
<b>Bund</b>	1	-
<b>Burgenland</b>	0,10	-
<b>Kärnten</b>	1	-
<b>Niederösterreich</b>	0,14	-
<b>Oberösterreich</b>	0,75	-
<b>Salzburg</b>	0,30	-
<b>Steiermark</b>	0,50	-
<b>Tirol</b>	0,85	-
<b>Vorarlberg</b>	0,45	-
<b>Wien</b>	1	EUR 190.000,-

\* Es handelt sich hierbei um Angaben des Bundesministeriums für Finanzen und der jeweils zuständigen Ämter der Landesregierungen, welche mangels exakter Quantifizierbarkeit überwiegend auf Schätzungen beruhen.

# Sektorrisikoanalyse Gewerbe

<b>Vermittlung von Lebensversicherungen und Versicherungsanlageprodukten</b>
<b>Allgemeine Informationen</b>
Bei dem Sektor handelt es sich um ein reglementiertes Gewerbe gemäß § 94 Z 76 GewO 1994. Die Einbeziehung unter die Vorschriften zur Bekämpfung von GW/TF erfolgt durch § 365m1 Abs. 1 Z 4 GewO 1994. In den Vollzugsberichten der Gewerbebehörden für 2019 wurde von ca. 11.000 betroffenen Unternehmen ausgegangen. Alle zwei Jahre erfolgt eine Risikoerhebung (insges. bis zu 40.000 Unternehmen). Zwecks möglichst einfacher Vorgehensweise in der Anfangsphase der Risikoerhebung erfolgte bisher keine Unterscheidung hins. Geldwäsche und Terrorismusfinanzierung, diese ist für die Zukunft jedoch vorgesehen. Die Feststellung der Bedrohungen in kriminalistischer und typologischer Hinsicht erfolgen derzeit im Wesentlichen aufgrund der Ergebnisse und Hinweise aus der SNRA und der NRA sowie der Strafverfolgungsbehörden. Primäre Aufgabe der Gewerbebehörden ist die Überwachung der Einhaltung des Verwaltungsrechts.
<b>Bedrohung</b>
<b>Terrorismusfinanzierung:</b> In den zusammengefassten Szenarien der SNRA wurde die Bedrohung dieses Sektors durch den Missbrauch für Zwecke der Terrorismusfinanzierung als mittel (2) angesehen. Gründe dafür sind die Komplexität der Produkte und die aufwendige erforderliche Planung.
<b>Geldwäscherei:</b> In den zusammengefassten Szenarien der SNRA wurde die Bedrohung mit einem mittleren Risiko (2) eingestuft. Grund ist die aufwendige Planung, die notwendig ist, um die Versicherungen zur Geldwäsche einzusetzen, darum gibt es wenige Fälle. Unter Einbeziehung der von den Gewerbebehörden durchgeführten Risikoanalyse ergibt sich als
<b>Bedrohung AT: 2</b> (2; Berechnung siehe Anhang)
<b>Verletzbarkeit</b>
<b>Terrorismusfinanzierung:</b> In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit des Sektors der Versicherungsvermittler als niedrig/mittel (1-2) eingestuft. Grund ist die Unattraktivität des Produktes für Zwecke der Terrorismusfinanzierung.
<b>Geldwäscherei:</b> In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von Versicherungsvermittlern im Hinblick auf den Missbrauch für die Zwecke der Geldwäscherei als niedrig/mittel (1-2) eingestuft. Unter Einbeziehung der von den Gewerbebehörden durchgeführten Risikoanalyse ergibt sich als
<b>Verletzbarkeit AT: 1-2</b> (1,5 Berechnung siehe Anhang)
<b>(a) Risikopotential:</b> Es wurden bisher keine Szenarien bekannt, die im Bereich der TF die Einbeziehung von Versicherungsvermittlern nahelegen. Durch nun konzipierte, noch zielgerichtete

Risikoerhebungsunterlagen, kontinuierliche Weiterverfolgung von Kontrollmaßnahmen, allenfalls verknüpft mit der Verhängung von in der Gewerbeordnung vorgesehenen Sanktionen, kann das Risikopotential weiter gesenkt werden. Ein weiterer Ansatz kann auch die weitere Vertiefung des Know-how der Gewerbebehörden darstellen.

**(b) Risikobewusstsein:**

Im Rahmen von umfangreichen Maßnahmen durch die Gewerbebehörde, wie Risikoerhebungen, Kontrollmaßnahmen, udgl. konnte ein verstärktes Bewusstsein für die Risiken in der Branche erreicht werden.

**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Bei dem Sektor handelt es sich um ein reglementiertes Gewerbe gemäß § 94 Z 76 GewO 1994. Die Einbeziehung unter die Vorschriften zur Bekämpfung von GW/TF erfolgt durch § 365m1 Abs. 1 Z 4 GewO 1994 und bezieht sich auf Lebensversicherungen und andere Dienstleistungen mit Anlagezweck; ausgenommen sind Versicherungsagenten, wenn sie keine Gelder entgegennehmen und entweder als Einfachagent oder im Umfang der Nebentätigkeit oder eines Nebengewerbes tätig werden. Die Aufsicht hat gem. § 338 GewO 1994 umfangreiche Möglichkeiten zur Vornahme von Überprüfungen. GW/TF sind Inhalt der jeweiligen Befähigungsprüfungen. Die im Bereich der Vollziehung der GW/TF - Bestimmungen zum Einsatz kommende Personalressource betrug 2019/2020 für den gesamten Gewerbebereich (Länder, BMDW) 10,72 Vollzeitäquivalente (zugezogen werden können bei Bedarf Sicherheitsorgane, vgl. § 336 Abs. 1 GewO 1994). Im Jahr 2020 ergab sich das Problem, dass die Bezirksverwaltungsbehörden auch für die Pandemiebekämpfung zu COVID 19 zuständig sind und Personal aus allen Zuständigkeitsbereichen dorthin einbezogen wurde.

**Risikomindernde Maßnahmen**

Verbesserung der Risikoerhebung, insbesondere Angabe der Risikokategorien, kontinuierliche Weiterverfolgung und -entwicklung der Aufsicht; präzisere Rückmeldung hinsichtlich der Verwaltungsdelikte; Zusammenarbeit mit anderen Behörden, soweit dies Datenschutzaspekte zulassen.

**Gesamtrisiko**

= 1-2 (1,7; Berechnung siehe Anhang)

**Empfehlungen**

Verbesserte Schulung, verstärkte Vollzugstätigkeit, Zusammenarbeit mit anderen Behörden wie etwa FMA und Finanzämter. Weitere Empfehlungen der EK, wie insbesondere hinsichtlich Vor-Ort-Kontrollen und themenbezogene Prüfungen speziell zum wirtschaftlichen Eigentümer.

## Bürodienstleister, Unternehmensberater

### Allgemeine Informationen

Daten: Ausführende der in Art. 2 Abs. 1 Z 3 lit c iVm Art. 3 Z 7 GW-RL genannten unternehmerischen Tätigkeiten, entspricht bestimmten Teiltätigkeiten der reglementierten Gewerbe Unternehmensberater nach § 94 Z 74 GewO 1994 sowie dem freien Gewerbe Büroarbeiten bzw. Büroservice (§ 365m1 Abs. 2 Z 3 GewO 1994), sofern diese die in der Richtlinie genannten Tätigkeiten ausüben. Etwas über 25.000 Unternehmen, allerdings verringert sich betreffend die Vollziehung diese Zahl, da als Ergebnis der Auswertung der Risikoerhebung und von div. Kontrolltätigkeiten viele der entsprechenden Gewerbeinhaber keine der relevanten insbesondere gründungsbezogenen Tätigkeiten ausüben, was in der Risikoerhebung berücksichtigt wird. Alle zwei Jahre erfolgt eine Risikoerhebung (insgesamt bis zu 40.000 Unternehmen). Zwecks möglichst einfacher Vorgehensweise in der Anfangsphase der Risikoerhebung erfolgte bisher keine Unterscheidung hins. Geldwäsche und Terrorismusfinanzierung, diese ist für die Zukunft jedoch vorgesehen. Die Feststellung der Bedrohungen in kriminalistischer und typologischer Hinsicht erfolgen derzeit im Wesentlichen aufgrund der Ergebnisse und Hinweise aus der SNRA und der NRA sowie der Strafverfolgungsbehörden. Primäre Aufgabe der Gewerbebehörden ist die Überwachung der Einhaltung des Verwaltungsrechts.

### Bedrohung

#### Terrorismusfinanzierung:

In den zusammengefassten Szenarien der SNRA wurde von der EK festgestellt, dass von terroristischen Organisationen keine Präferenz für derartige Vorgänge als Mittel der Finanzierung besteht, sodass die Bedrohung mit mittel (2) bewertet wird.

#### Geldwäscherei:

In den zusammengefassten Szenarien der SNRA wurden die gegenständlichen Aktivitäten als typisches Vehikel für Geldwäsche identifiziert und ein generell sehr hohes Bedrohungsrisiko (4) gesehen, dass dieser Sektor für Geldwäsche missbraucht wird. Unter Einbeziehung der von den Gewerbebehörden durchgeführten Risikoanalyse ergibt sich als

**Bedrohung AT: 2 - 3** (2,6; Berechnung siehe Anhang)

### Verletzbarkeit

#### Terrorismusfinanzierung:

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit dieses Sektors als hoch (3) eingestuft.

#### Geldwäscherei:

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit dieses Sektors im Hinblick auf den Missbrauch für die Zwecke der Geldwäscherei als hoch/sehr hoch (3-4) eingestuft, insbesondere wegen Lücken bei der Feststellung des wirtschaftlichen Eigentümers. Unter Einbeziehung der von den Gewerbebehörden durchgeführten Risikoanalyse ergibt sich als

**Verletzbarkeit AT: 2-3** (2,8; Berechnung siehe Anhang)

#### (a) Risikopotential:

Entsprechend auch den Aussagen in der SNRA kann generell nicht ausgeschlossen werden, dass Identifizierungserfordernisse bei der Gründung von Gesellschaften oder Zurverfügungstellung von Büroserviceleistungen umgangen werden können. Ein Risiko aufgrund der Größe des Sektors relativiert sich dadurch, dass gemäß Ergebnis der Auswertung der Risikoerhebung und von div. Kontrolltätigkeiten viele der betroffenen Gewerbeberechtigten keine



der einschlägig der GW-RL unterliegenden Tätigkeiten ausüben. Durch nun konzipierte, noch zielgerichtetere Risikoerhebungsunterlagen, kontinuierliche Weiterverfolgung von Kontrollmaßnahmen, allenfalls verknüpft mit der Verhängung von in der Gewerbeordnung vorgesehenen Sanktionen, kann das Risikopotential weiter gesenkt werden. Ein weiterer Ansatz kann auch die weitere Vertiefung des Know-how der Gewerbebehörden darstellen.

**(b) Risikobewusstsein:**

Im Rahmen von umfangreichen Maßnahmen durch die Gewerbebehörde, wie Risikoerhebungen, Kontrollmaßnahmen, udgl. konnte ein verstärktes Bewusstsein für die Risiken in der Branche erreicht werden.

**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Tätigkeit des Unternehmensberaters ist nach § 94 Z 74 GewO 1994 ein reglementiertes Gewerbe. Gewerbezugang erfordert Ausbildungsnachweis, Ausbildung umfasst GW/TF. Die im Sinne der Geldwäscherichtlinie einschlägigen Tätigkeiten sowie die Tätigkeiten der Büroserviceunternehmen unterliegen den Bestimmungen der GewO 1994 zu GW/TF. Die im Bereich der Vollziehung der GW/TF - Bestimmungen zum Einsatz kommende Personalressource betrug 2019/2020 für den gesamten Gewerbebereich (Länder, BMDW) 10,72 Vollzeitäquivalente (zugezogen werden können bei Bedarf Sicherheitsorgane, vgl. § 336 Abs. 1 GewO 1994). Im Jahr 2020 ergab sich das Problem, dass die Bezirksverwaltungsbehörden auch für die Pandemiebekämpfung zu COVID 19 zuständig sind und Personal aus allen Zuständigkeitsbereichen dorthin einbezogen wurde.

**Risikomindernde Maßnahmen**

Verbesserung der Risikoerhebung, insbesondere Angabe der Risikokategorien, kontinuierliche Weiterverfolgung und -entwicklung der Aufsicht; präzisere Rückmeldung hinsichtlich der Verwaltungsdelikte; Zusammenarbeit mit anderen Behörden, soweit dies Datenschutzaspekte zulassen.

**Gesamtrisiko**

= 2-3 (2,7; Berechnung siehe Anhang)

**Empfehlungen**

Verbesserte Schulung, verstärkte Vollzugstätigkeit, Zusammenarbeit mit anderen Behörden wie etwa FMA und Finanzämter. Befolgung der Empfehlungen der EK, wie insbesondere hinsichtlich Vor-Ort-Kontrollen und themenbezogene Prüfungen speziell zum wirtschaftlichen Eigentümer.

**Handel einschließlich Versteigerer**

**Allgemeine Informationen**

Daten: Handelssektor in Österreich mit ca. 210.000 Unternehmen; es erfolgt eine risikobezogene Fokussierung auf Handel mit wertvollen Gütern wie Gold und Edelsteine, Juweliere, Antiquitätenhandel, Autohandel, Kunsthandel, Tabakgroßhandel, Ölhandel, Waffenhandel, Kulturguthandel u.a. lt. Anhang III GW-RI. Effektiv betroffen Unternehmen, wenn generell Bargeschäfte ab 10.000 € tätigen, bzw. Kunsthandel oder Lagerung von Kunstwerken auch bei unbaren Geschäften dieser Größenordnung. Lt. Vollzugsberichten 2019 etwas über 16.000 Handelsbetriebe betroffen.

Alle zwei Jahre erfolgt Risikoerhebung (insgesamt bis zu 40.000 Unternehmen). Zwecks möglichst einfacher Vorgehensweise in der Anfangsphase der Risikoerhebung erfolgte bisher keine Unterscheidung hins. Geldwäsche und Terrorismusfinanzierung, diese ist für die Zukunft jedoch vorgesehen. Die Feststellung der Bedrohungen in kriminalistischer und typologischer Hinsicht erfolgen derzeit im Wesentlichen aufgrund der Ergebnisse und Hinweise aus der SNRA und der NRA sowie der Strafverfolgungsbehörden. Primäre Aufgabe der Gewerbebehörden ist die Überwachung der Einhaltung des Verwaltungsrechts.

### Bedrohung

#### **Terrorismusfinanzierung:**

In den zusammengefassten Szenarien der SNRA wurde generell ein Risiko gesehen, dass Händler für terroristische Aktivitäten missbraucht werden. Die SNRA unterscheidet (staff document) speziell einerseits nach Handel mit Kunst und Antiquitäten (2) und andererseits Edelmetall und Edelsteinen (2-3) sowie sonstigen Gütern mit hohem Einzelwert (z.B. Autos, Boote, Schmuck) (nicht relevant).

#### **Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Bedrohung hinsichtlich Handel mit Gold und Diamanten mit einem sehr hohen Risiko (4) eingestuft, da Gold und Diamanten leicht über die Grenzen transportiert werden können. Ferner bestehen umfangreiche Geldwäschekonstruktionen in den Bereichen Handel mit Kunst und Antiquitäten (Risiko 2) und sonstige Güter mit hohem Einzelwert (Risiko 4). Unter Einbeziehung der von den Gewerbebehörden durchgeführten Risikoanalyse ergibt sich als

**Bedrohung AT: 2** (Kunst, Antiquitäten); **3** (Edelmetall, Edelsteine), **2-3** (2,4 andere wertvolle Güter); Berechnung siehe Anhang

### Verletzbarkeit

#### **Terrorismusfinanzierung:**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von Händlern im Hinblick auf den Missbrauch des Handels mit Gold und Diamanten für die Zwecke der Terrorismusfinanzierung als hoch (3) eingestuft. Bei Artefakten und Antiquitäten wird die Verletzbarkeit wegen des mangelnden Bewusstseins betreffend diese Gefahr als hoch/sehr hoch (3-4) eingestuft. (sonstige Güter mit hohem Einzelwert: nicht relevant).

#### **Geldwäscherei:**

In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von Händlern im Hinblick auf den Missbrauch des Handels mit Gold und Diamanten für die Zwecke der Geldwäsche als hoch (3) eingestuft. Dasselbe Risiko besteht gemäß SNRA im Bereich des Handels mit anderen Luxusgütern als Gold, Diamanten und Antiquitäten, nämlich etwa Autos, Schmuck oder Luxusyachten (3). Hinsichtlich Antiquitäten und Artefakten wird die Verletzbarkeit hinsichtlich Missbrauch zur Geldwäsche als hoch/sehr hoch angesehen (3-4). Unter Einbeziehung der von den Gewerbebehörden durchgeführten Risikoanalyse ergibt sich als

**Verletzbarkeit AT: 3-4** (3,2 Kunst, Antiquitäten); **2-3** (2,9 Edelmetall, Edelsteine); **2-3** (2,2 andere wertvolle Güter); Berechnung siehe Anhang

#### **(a) Risikopotential:**

Ein Risiko besteht speziell im Falle des Handels aufgrund der Größe des Sektors. Derzeit bestehen weiter die Bargeldgrenzen von 10.000 € gemäß der EU-GW-Richtlinie. Dabei sind auch zusammenhängende Transaktionen für die Pflichten der Gewerbetreibenden relevant. Durch nun konzipierte, noch zielgerichtetere Risikoerhebungsunterlagen, kontinuierliche Weiterverfolgung von Kontrollmaßnahmen, allenfalls verknüpft mit der Verhängung von in

der Gewerbeordnung vorgesehenen Sanktionen, kann das Risikopotential weiter gesenkt werden. Ein weiterer Ansatz kann auch die weitere Vertiefung des Know - how der Gewerbebehörden darstellen.

**(b) Risikobewusstsein:**

Im Rahmen von umfangreichen Maßnahmen durch die Gewerbebehörde, wie Risikoerhebungen, Kontrollmaßnahmen udgl., konnte ein verstärktes Bewusstsein für die Risiken in der Branche erreicht werden.

**(c) Rechtliche Rahmenbedingungen und Aufsicht/Governance:**

Im Gewerberecht bestehen die generellen Anforderungen an die Gewerbetreibenden, Registrierung, Freiheit von Vorstrafen und Konkursfreiheit. Bargeschäfte ab 10.000€ sowohl im Ankauf wie auch im Verkauf lösen die Verpflichtungen aus. Die Gewerbebehörden haben volle Kontrollrechte hinsichtlich Einschau in Geschäftsunterlagen und Betriebsstätten aufgrund § 338 GewO 1994. Aufgrund der Umsetzung der fünften EU-Geldwäscherichtlinie (EU) 2018/843 durch BGBl. I. Nr. 111/2019 wurden nunmehr auch Kunsthändler ausdrücklich in den Kreis der Verpflichteten einbezogen. Bei diesen erfolgt die Einbeziehung nunmehr ab einer Grenze von 10.000 €, auch bei unbaren Geschäften. Ausdrücklich als erhöht gefährdet werden im Gewerberecht (Anlage 8 zur Gewerbeordnung) der Tabakgroßhandel, Ölhandel, Waffenhandel, Kulturguthandel und der Handel mit anderen Artikeln besonderer Bedeutung genannt. Die im Bereich der Vollziehung der GW/FT - Bestimmungen zum Einsatz kommende Personalressource betrug 2019/2020 für den gesamten Gewerbebereich (Länder, BMDW) 10,72 Vollzeitäquivalente (zugezogen werden können bei Bedarf Sicherheitsorgane, vgl. § 336 Abs. 1 GewO 1994). Im Jahr 2020 ergab sich das Problem, dass die Bezirksverwaltungsbehörden auch für die Pandemiebekämpfung zu COVID 19 zuständig sind und Personal aus allen Zuständigkeitsbereichen dorthin einbezogen wurde.

**Risikomindernde Maßnahmen**

Verbesserung der Risikoerhebung, insbesondere Angabe der Risikokategorien, kontinuierliche Weiterverfolgung und -entwicklung der Aufsicht; präzisere Rückmeldung hinsichtlich der Verwaltungsdelikte; Zusammenarbeit mit anderen Behörden, soweit dies Datenschutzaspekte zulassen.

**Gesamtrisiko**

= 2-3 (2,7 Kunst, Antiquitäten; 2,9 Edelmetall, Edelsteine; 2,3 andere); Berechnung siehe Anhang

**Empfehlungen**

Verbesserte Schulung, verstärkte Vollzugstätigkeit, Zusammenarbeit mit anderen Behörden wie etwa FMA und Finanzämter. Befolgung der Empfehlungen der EK, wie insbesondere hinsichtlich Vor-Ort-Kontrollen und themenbezogene Prüfungen speziell zum wirtschaftlichen Eigentümer.

**Immobilienmakler**

**Allgemeine Informationen**

Bei dem Sektor handelt es sich um ein reglementiertes Gewerbe nach § 94 Z 35 der Gewerbeordnung 1994. Für den Gewerbezugang sind umfangreiche Ausbildungserfordernisse gegeben; diese enthalten auch Ausbildungen im Bereich Verwaltungsrecht, somit auch GW/TF.

<p>Im Zuge der Vollziehung im Jahre 2019 wurde eine Anzahl betroffener Betriebe von etwa 6.000 festgestellt. Alle zwei Jahre erfolgt eine Risikoerhebung (insgesamt bis zu 40.000 Unternehmen). Zwecks möglichst einfacher Vorgehensweise in der Anfangsphase der Risikoerhebung erfolgte bisher keine Unterscheidung hins. Geldwäsche und Terrorismusfinanzierung, diese ist für die Zukunft jedoch vorgesehen. Die Feststellung der Bedrohungen in kriminalistischer und typologischer Hinsicht erfolgen derzeit im Wesentlichen aufgrund der Ergebnisse und Hinweise aus der SNRA und der NRA sowie der Strafverfolgungsbehörden. Primäre Aufgabe der Gewerbebehörden ist Überwachung der Einhaltung des Verwaltungsrechts.</p>
<p><b>Bedrohung</b></p>
<p><b>Terrorismusfinanzierung:</b>  In den zusammengefassten Szenarien der SNRA wurde ein Risiko der Terrorismusfinanzierung in Verbindung mit häufig stattfindenden Geldwäschevorgängen gesehen, bei denen Investitionen in Immobilien stattfinden, um den illegalen Ursprung von Vermögenswerten zu verschleiern. Das Risiko, dass Immobilienmakler für Terrorismusfinanzierung missbraucht werden, wurde im Gleichklang mit dem Geldwäscherisiko als sehr hoch (4) angesehen.</p>
<p><b>Geldwäscherei:</b>  In den zusammengefassten Szenarien der SNRA wurde ein wesentliches Risiko dieses Sektors erkannt und zwar in Verbindung mit anderen Sektoren, wie TCSP und die Bedrohung mit einem sehr hohen Risiko (4) eingestuft. Unter Einbeziehung der von den Gewerbebehörden durchgeführten Risikoanalyse ergibt sich als</p> <p><b>Bedrohung AT: 3-4</b> (3,2; Berechnung siehe Anhang)</p>
<p><b>Verletzbarkeit</b></p>
<p><b>Terrorismusfinanzierung:</b>  In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit als ausschließlich im Zusammenhang mit Geldwäschevorgängen gesehen, sodass eine separate Analyse unterblieb und die Verletzbarkeit als sehr hoch (4) eingestuft.</p>
<p><b>Geldwäscherei:</b>  In den zusammengefassten Szenarien der SNRA wurde die Verletzbarkeit von Immobilienmaklern im Hinblick auf den Missbrauch für die Zwecke der Geldwäscherei als hoch/sehr hoch (3-4) eingestuft. Unter Einbeziehung der von den Gewerbebehörden durchgeführten Risikoanalyse ergibt sich als</p> <p><b>Verletzbarkeit AT: 3-4</b> (3,1; Berechnung siehe Anhang)</p>
<p><b>Risikomindernde Maßnahmen</b></p>
<p>Verbesserung der Risikoerhebung, insbesondere Angabe der Risikokategorien, kontinuierliche Weiterverfolgung und -entwicklung der Aufsicht; präzisere Rückmeldung hinsichtlich der Verwaltungsdelikte; Zusammenarbeit mit anderen Behörden, soweit dies Datenschutzaspekte zulassen.</p>
<p><b>Gesamtrisiko</b></p>
<p>= <b>3 - 4</b> (3,1; Berechnung siehe Anhang; Hinweis: von der WKÖ wurde bei diesem Sektor von einem mittleren bis hohen Risiko ausgegangen; der errechnete Risikowert von 3,1 - somit nur knapp über drei - bestätigt dies in der Tendenz).</p>
<p><b>Empfehlungen</b></p>

Verbesserte Schulung, verstärkte Vollzugstätigkeit, Zusammenarbeit mit anderen Behörden wie etwa FMA und Finanzämter. Weitere Empfehlungen der EK, wie insbesondere hinsichtlich Vor-Ort-Kontrollen und themenbezogene Prüfungen speziell zum wirtschaftlichen Eigentümer.

## Anhang

### Allgemeine Informationen

Auf den nächsten Seiten werden die detaillierten Risikowerte und deren Berechnung dargestellt (AT Risikozahlen, Korr.Fakt. grdstzl. +1, SNRA Obergrenze, AT Risikozahl Untergrenze; Abkürzungen: Bedr. TF - SNRA - Bedrohung Terrorismusfinanzierung gem. SNRA 2019; Bedr. TF - Gewb - Bedrohung Terrorismusfinanzierung gem. Erhebung Gewerbebehörden; Bedr. GW - SNRA - Bedrohung Geldwäsche gem. SNRA 2019; Bedr. GW - Gewb - Bedrohung Geldwäsche gem. Erhebung Gewerbebehörden; Bedr. ges. - Bedrohung gesamt; Verl. TF - SNRA - Verletzbarkeit Terrorismusfinanzierung gem. SNRA 2019; Verl. TF - Gewb - Verletzbarkeit Terrorismusfinanzierung gem. Erhebung Gewerbebehörden; Verl. GW - SNRA - Verletzbarkeit Geldwäsche gem. SNRA 2019; Verl. GW - Gewb - Verletzbarkeit Geldwäsche gem. Erhebung Gewerbebehörden; Verl. ges. - Verletzbarkeit gesamt).

	Tätigkeit gem. SNRA	Gewerbe nach GewO		Tätigkeit gem. SNRA	Gewerbe nach GewO			
	life insurance	Versicherungsvermittlung		TCSP	Unternehmensberater, Büroserviceunternehmen			
Bedr. TF - SNRA	2,0		Bedr. TF - SNRA	2,0				
Bedr. TF - Gewb	2,0		Bedr. TF - Gewb	2,0				
Durchschnitt	2,0		Durchschnitt	2,0				
Bedr. GW - SNRA	2,0		Bedr. GW - SNRA	4,0				
Bedr. GW - Gewb	2,0		Bedr. GW - Gewb	2,3				
Durchschnitt	2,0		Durchschnitt	3,2				
Bedr. ges.	2,0		Bedr. ges.	2,6				
Verl. TF - SNRA	1,5		Verl. TF - SNRA	3,0				
Verl. TF - Gewb	1,5		Verl. TF - Gewb	2,3				
Durchschnitt	1,5		Durchschnitt	2,7				
Verl. GW - SNRA	1,5		Verl. GW - SNRA	3,5				
Verl. GW - Gewb	1,5		Verl. GW - Gewb	2,3				
Durchschnitt	1,5		Durchschnitt	2,9				
Verl. ges.	1,5		Verl. ges.	2,8				
Gesamtwert	1,7		Gesamtwert	2,7				
Risikostufe	niedrig-mittel		Risikostufe	mittel-hoch				
	Tätigkeit gem. SNRA	Gewerbe nach GewO		Tätigkeit gem. SNRA	Gewerbe nach GewO			
	hv goods-artefacts, antiquities	Handel		hv assets-precious metals, stones	Handel			
Bedr. TF - SNRA	2,0		Bedr. TF - SNRA	2,5				
Bedr. TF - Gewb	2,0		Bedr. TF - Gewb	2,5				
Durchschnitt	2,0		Durchschnitt	2,5				
Bedr. GW - SNRA	2,0		Bedr. GW - SNRA	4,0				
Bedr. GW - Gewb	2,0		Bedr. GW - Gewb	2,8				
Durchschnitt	2,0		Durchschnitt	3,4				
Bedr. ges.	2,0		Bedr. ges.	3,0				
Verl. TF - SNRA	3,5		Verl. TF - SNRA	3,0				
Verl. TF - Gewb	2,8		Verl. TF - Gewb	2,8				
Durchschnitt	3,2		Durchschnitt	2,9				
Verl. GW - SNRA	3,5		Verl. GW - SNRA	3,0				
Verl. GW - Gewb	2,8		Verl. GW - Gewb	2,8				
Durchschnitt	3,2		Durchschnitt	2,9				
Verl. ges.	3,2		Verl. ges.	2,9				
Gesamtwert	2,7		Gesamtwert	2,9				
Risikostufe	mittel-hoch		Risikostufe	mittel-hoch				

	Tätigkeit gem. SNRA	Gewerbe nach GewO		Tätigkeit gem. SNRA	Gewerbe nach GewO
	hv assets-other than prec. met.	Handel		Investment real estate	Immobilienmakler
Bedr. TF - SNRA	1,0		Bedr. TF - SNRA	4,0	
Bedr. TF - Gewb	1,8		Bedr. TF - Gewb	2,4	
Durchschnitt	1,4		Durchschnitt	3,2	
Bedr. GW - SNRA	4,0		Bedr. GW - SNRA	4,0	
Bedr. GW - Gewb	2,8		Bedr. GW - Gewb	2,4	
Durchschnitt	3,4		Durchschnitt	3,2	
Bedr. ges.	2,4		Bedr. ges.	3,2	
Verl. TF - SNRA	1,0		Verl. TF - SNRA	4,0	
Verl. TF - Gewb	1,8		Verl. TF - Gewb	2,4	
Durchschnitt	1,4		Durchschnitt	3,2	
Verl. GW - SNRA	3,0		Verl. GW - SNRA	3,5	
Verl. GW - Gewb	2,8		Verl. GW - Gewb	2,4	
Durchschnitt	2,9		Durchschnitt	3,0	
Verl. ges.	2,2		Verl. ges.	3,1	
Gesamtwert	2,3		Gesamtwert	3,1	
Risikostufe	mittel-hoch		Risikostufe	hoch-sehr hoch	

# Schlusswort

Die **Nationale Risikoanalyse** ist das **gemeinsame Ergebnisdokument** aller mit der Prävention und Bekämpfung von Geldwäscherei und Terrorismusfinanzierung in Österreich befasster Behörden. Sie trägt der **stetigen Entwicklung des europäischen und internationalen Rechtsrahmens** und der **Länderprüfung Österreichs durch die FATF Rechnung**. Neben der Berücksichtigung von neuen Verpflichteten und geänderten gesetzlichen Vorgaben stützt sich die Methodologie auf **quantitative und qualitative Faktoren**, die durch **Typologien** und **Fallstudien** illustriert werden.

Auf Basis einer **gemeinsamen Vorlage und Methodologie** erstellten die Mitglieder des Nationalen Koordinierungsgremiums einen Erstentwurf ihrer Sektorrisikoanalysen. Die Erstentwürfe wurden an das Bundesministerium für Inneres zum **Abgleich mit operativen Erkenntnissen** übermittelt. Unter Berücksichtigung der **Rückmeldungen des Bundesministeriums für Inneres** und des **Privatsektors** erfolgte die Erstellung der Letztentwürfe und die Konsolidierung in dem Ergebnisdokument. Dieses stützt sich auf die **Expertise aller österreichischen Akteure** der Prävention und Bekämpfung von Geldwäscherei und Terrorismusfinanzierung.

Die Nationale Risikoanalyse dient zur **Ermittlung**, zur **Bewertung**, zum **Verständnis** und zur **Minderung** der im **Inland bestehenden Risiken der Geldwäscherei und Terrorismusfinanzierung**.

Die **Ermittlung** und **Bewertung** der **Risiken** wird durch den breit gespannten Bogen der Nationalen Risikoanalyse unterstützt. Einerseits bieten **Analysen der Vortaten**, des **wirtschaftlichen Eigentums** und der **Betrugsbekämpfung** ein **breites Panorama der Bedrohungen**. Andererseits zeichnen die Sektorrisikoanalysen ein **differenziertes Bild der Risikolandschaft**. Hervorzuheben ist, dass sich die Risiken der Geldwäscherei und Terrorismusfinanzierung in Bezug auf einzelne Produkte und Dienstleistungen sowie zwischen den Sektoren unterscheiden.

Durch ihre detaillierte Darstellung der Risikolandschaft trägt die Nationale Risikoanalyse außerdem zum **Verständnis** und zur Setzung von Maßnahmen zur **Minderung der Risiken** durch die Verpflichteten bei. Die befassten Behörden formulierten auf Basis der von Ihnen festgestellten Risiken Empfehlungen für weitere Maßnahmen zur Minderung der **bestehenden Risiken der Geldwäscherei und Terrorismusfinanzierung**.

Die Nationale Risikoanalyse setzt einen **wichtigen Schritt zur Prävention von Geldwäscherei und Terrorismusfinanzierung** in Österreich. Das Bundesministerium für Finanzen bekennt sich zur **Umsetzung** der **internationalen und europäischen Standards** zur Geldwäschereibekämpfung und deren stetiger **Fortentwicklung** mit seinen europäischen und internationalen Partnern.



# Abkürzungsverzeichnis

Abs.	<i>Absatz</i>
AltFG	<i>Alternativfinanzierungsgesetz</i>
Art.	<i>Artikel</i>
BAO	<i>Bundesabgabenordnung</i>
BGBI	<i>Bundesgesetzblatt</i>
BiBuG	<i>Bilanzbuchhaltungsgesetz</i>
BWG	<i>Bankwesengesetz</i>
BVT	<i>Bundesamt für Verfassungsschutz und Terrorismusbekämpfung</i>
CESEE	<i>Central, Eastern and Southeastern Europe</i>
EK	<i>Europäische Kommission</i>
EU	<i>Europäische Union</i>
EU-MPFG	<i>EU-Meldepflichtgesetz</i>
FATF	<i>Financial Action Task Force</i>
FI	<i>Finanzinstitut</i>
FinStrG	<i>Finanzstrafgesetz</i>
FIU	<i>Financial Intelligence Unit (Geldwäschemeldestelle)</i>
FMA	<i>Finanzmarktaufsichtsbehörde</i>
FM-GwG	<i>Finanzmarkt-Geldwäschegesetz</i>
GewO	<i>Gewerbeordnung</i>
GMSG	<i>Gemeinsamer Meldestandard-Gesetz</i>
GSPG	<i>Glücksspielgesetz</i>
gem.	<i>gemäß</i>
grdstzl.	<i>grundsätzlich</i>
GW	<i>Geldwäscherei</i>
hins.	<i>hinsichtlich</i>
iSd	<i>im Sinne des</i>
KI	<i>Kreditinstitut</i>
lit.	<i>Litera (Buchstabe)</i>
MS	<i>Mitgliedstaat (der Europäischen Union)</i>
NO	<i>Notariatsordnung</i>
Nr.	<i>Nummer</i>
NRA	<i>Nationale Risikoanalyse</i>
OeNB	<i>Oesterreichische Nationalbank</i>
RAO	<i>Rechtsanwaltsordnung</i>
RI	<i>Richtlinie</i>
SNRA	<i>Supranationale Risikoanalyse</i>
SMG	<i>Suchtmittelgesetz</i>
StGB	<i>Strafgesetzbuch</i>
sublit.	<i>Sublitera (Unterbuchstabe)</i>
SWD	<i>Staff Working Document</i>
TF	<i>Terrorismusfinanzierung</i>
VBÄ	<i>Vollbeschäftigtenäquivalente</i>
VO	<i>Verordnung</i>
WAG	<i>Wertpapieraufsichtsgesetz</i>

WiReG	<i>Wirtschaftliche Eigentümer Register bzw. Wirtschaftliche Eigentümer Registergesetz</i>
WKÖ	<i>Wirtschaftskammer Österreich</i>
WTBG	<i>Wirtschaftstreuhandberufsgesetz</i>
Z	<i>Ziffer</i>
zB	<i>zum Beispiel</i>

**Bundesministerium für Finanzen**

Johannesgasse 5, 1010 Wien

+43 1 514 33-0

[email@bmf.gv.at](mailto:email@bmf.gv.at)

[bmf.gv.at](http://bmf.gv.at)