

Dokumentennummer:

Veröffentlichungsdatum:

# FMA-RUNDSCHREIBEN

## Risikoanalyse

### ZUR PRÄVENTION VON GELDWÄSCHEREI UND TERRORISMUSFINANZIERUNG

Stand: ENTWURF – Externe Konsultation

Disclaimer: Dieses Rundschreiben stellt keine Verordnung dar. Es soll als Orientierungshilfe dienen und gibt die Rechtsauffassung der FMA wieder. Über die gesetzlichen Bestimmungen hinausgehende Rechte und Pflichten können aus Rundschreiben nicht abgeleitet werden.

# INHALTSVERZEICHNIS

INHALTSVERZEICHNIS.....	3
1 Einleitung.....	5
2 Nationale Risikoanalyse .....	9
2.1 Einleitung.....	9
2.2 Inhalt .....	9
2.3 Vorfällen, Methoden, Bedrohungen und Risiken .....	10
2.4 Ausführungen und Ergebnisse zum Finanzmarkt.....	11
3 Risikoanalyse auf Unternehmensebene.....	13
3.1 Allgemeines und Methodik .....	13
3.2 Praktischer Leitfaden zur Erstellung.....	13
3.2.1 Schritt 1: Definition sämtlicher relevanter Risikofaktoren.....	14
3.2.2 Schritt 2: Analyse der definierten Risikofaktoren .....	15
3.2.3 Schritt 3: Bewertung der definierten Risikofaktoren .....	16
3.2.4 Schritt 4: Ableitung eines Gesamtrisikos auf Unternehmensebene .....	17
3.2.5 Schritt 5: Risikominimierende Maßnahmen .....	17
4 Risikoanalyse auf Einzelkundenebene .....	19
4.1 Identifizierung und Bewertung der Risiken von Geldwäscherei und Terrorismusfinanzierung .....	19
4.1.1 Erstellung des Risikoprofils.....	19
4.1.2 Anlage I.....	20
4.1.2.1 Zweck eines Kontos oder einer Geschäftsbeziehung.....	20
4.1.2.2 Höhe der von einem Kunden eingezahlten Vermögenswerte oder Umfang der ausgeführten Transaktionen .....	21
4.1.2.3 Regelmäßigkeit oder Dauer der Geschäftsbeziehung.....	21
4.1.3 Anlage II.....	21
4.1.3.1 Risikofaktoren bezüglich Kunden .....	22
4.1.3.2 Risikofaktoren bezüglich Produkte, Dienstleistungen, Transaktionen oder Vertriebskanäle .....	23
4.1.3.3 Risikofaktoren in geographischer Hinsicht.....	24
4.1.4 Anlage III.....	26
4.1.4.1 Risikofaktoren bezüglich Kunden .....	26

4.1.4.2	Risikofaktoren bezüglich Produkten, Dienstleistungen, Transaktionen oder Vertriebskanälen .....	28
4.1.4.3	Risikofaktoren in geographischer Hinsicht.....	29
4.1.5	Unternehmensspezifische Risikofaktoren.....	30
4.1.5.1	Exkurs: Risikofaktoren im Bereich virtueller Währungen .....	30
4.1.6	Gewichtung von Risikofaktoren .....	31
4.1.7	Risikoklassifizierung mittels automationsunterstützter Systeme .....	31
5	Anhang .....	33
5.1	Materialien .....	33

# 1 EINLEITUNG

- 1 Der risikoorientierte Ansatz in der Prävention von Geldwäscherei und Terrorismusfinanzierung bedeutet, dass von supranationalen Behörden, Staaten, zuständigen Behörden sowie Verpflichteten nach der Richtlinie (EU) 2018/843 (5. Geldwäsche RL) erwartet wird, dass Risiken der Geldwäscherei und Terrorismusfinanzierung, identifiziert, bewertet und verstanden werden. In der Folge sind verhältnismäßige – dem Risiko angemessene – Maßnahmen der Risikominimierung zu setzen.
- 2 Dieses Rundschreiben soll den Verpflichteten nach dem Finanzmarkt-Geldwäschegesetz (FM-GwG<sup>1</sup>) – in der Folge kurz „Verpflichtete“ – als Anleitung zur Ermittlung und Bewertung von potentiellen Risiken der Geldwäscherei und Terrorismusfinanzierung dienen.
- 3 Dieses Rundschreiben stellt keine Verordnung dar. Es soll als Orientierungshilfe dienen und gibt die Rechtsauffassung der FMA wieder. Über die gesetzlichen Bestimmungen hinausgehende Rechte und Pflichten können aus Rundschreiben nicht abgeleitet werden.
- 4 Verpflichtete des FM-GwG sind
  - Kreditinstitute gemäß § 1 Abs. 1 Bankwesengesetz (BWG<sup>2</sup>) und CRR-Kreditinstitute gemäß § 9 BWG, die Tätigkeiten im Inland über eine Zweigstelle erbringen;
  - Finanzinstitute gemäß § 1 Abs. 2 Z 1 bis 6 BWG (Rz 5);
  - Versicherungsunternehmen gemäß § 1 Abs. 1 Z 1 Versicherungsaufsichtsgesetz 2016 (VAG 2016<sup>3</sup>) und kleine Versicherungsunternehmen gemäß § 1 Abs. 1 Z 2 VAG 2016 jeweils im Rahmen des Betriebes der Lebensversicherung (Zweige 19 bis 22 gemäß Anlage A zum VAG 2016);
  - Wertpapierfirmen gemäß § 3 Abs. 1 Wertpapieraufsichtsgesetz 2018 (WAG 2018<sup>4</sup>) und Wertpapierdienstleistungsunternehmen gemäß § 4 Abs. 1 WAG 2018;
  - AIFM gemäß § 1 Abs. 5 und § 4 Abs. 1 Alternative Investmentfonds Manager-Gesetz (AIFMG<sup>5</sup>) und Nicht-EU-AIFM gemäß § 39 Abs. 3 AIFMG;
  - E-Geldinstitute gemäß § 3 Abs. 2 E-Geldgesetz 2010<sup>6</sup>;
  - Zahlungsinstitute gemäß § 10 Zahlungsdienstegesetz 2018 (ZaDiG 2018<sup>7</sup>);

---

<sup>1</sup> Finanzmarkt-Geldwäschegesetz (FM-GwG), BGBl. I Nr. 118/2016, in der geltenden Fassung.

<sup>2</sup> Bankwesengesetz (BWG), BGBl. Nr. 532/1993, in der geltenden Fassung.

<sup>3</sup> Versicherungsaufsichtsgesetz 2016 (VAG 2016), BGBl. I Nr. 34/2015, in der geltenden Fassung.

<sup>4</sup> Wertpapieraufsichtsgesetz 2018 (WAG 2018), BGBl. I Nr. 107/2017, in der geltenden Fassung.

<sup>5</sup> Alternative Investmentfonds Manager-Gesetz (AIFMG), BGBl. I Nr. 135/2013, in der geltenden Fassung.

<sup>6</sup> E-Geldgesetz 2010, BGBl. I Nr. 107/2010, in der geltenden Fassung.

<sup>7</sup> Zahlungsdienstegesetz 2018 (ZaDiG 2018), BGBl. I Nr. 17/2018, in der geltenden Fassung.

- die Post hinsichtlich ihres Geldverkehrs;
  - Finanzinstitute gemäß Art. 3 Z 2 lit. a bis d der Richtlinie (EU) 2015/849 („4. Geldwäsche-RL“) mit Sitz in einem anderen Mitgliedstaat mit dem über im Inland gelegene Zweigstellen bzw. Zweigniederlassungen ausgeübten Geschäftsbetrieb sowie im Inland gelegene Zweigstellen bzw. Zweigniederlassungen von solchen Finanzinstituten, die in Drittländern zugelassen sind;
  - Abbaueinheiten gemäß § 84 Abs. 2 Bundesgesetz über die Sanierung und Abwicklung von Banken (BaSAG<sup>8</sup>) sowie § 3 Abs. 4 Bundesgesetz zur Schaffung einer Abbaueinheit (GSA<sup>9</sup>);
  - Abbaugesellschaften gemäß § 162 Abs. 1 BaSAG iVm § 84 Abs. 2 BaSAG;
  - Dienstleister in Bezug auf virtuelle Währungen gemäß § 2 Z 22 FM-GwG (RZ 6).
- 5 Ein Finanzinstitut gemäß § 1 Abs. 2 Z 1 bis Z 6 BWG ist, wer kein Kreditinstitut iSd § 1 Abs. 1 BWG ist und berechtigt ist, eine oder mehrere der in § 1 Abs. 2 BWG aufgezählten Tätigkeiten gewerbsmäßig durchzuführen, sofern er diese als Haupttätigkeit betreibt. Die für die Qualifikation als Finanzinstitut begriffsbestimmende Haupttätigkeit ist aufgrund des sich im konkreten Einzelfall ergebenden Gesamtbildes, d.h. unter Berücksichtigung sämtlicher relevanter quantitativer und qualitativer Faktoren und Kriterien im Sinne eines beweglichen Systems zu ermitteln. Jedenfalls ist von einer Haupttätigkeit auszugehen, wenn diese Tätigkeit 50 % der Unternehmensleistung ausmacht.<sup>10</sup> Darüber hinaus ist das Vorliegen einer Haupttätigkeit nicht nur anhand des bloßen Beitrags zur Unternehmensleistung – also eines rein quantitativen Merkmals – zu beurteilen. Vielmehr ist aufgrund des Gesamtbildes im Einzelfall anhand qualitativer Merkmale zu beurteilen, ob es sich bei einer Tätigkeit eines Unternehmens um eine Haupttätigkeit handelt oder ob diese Tätigkeit *„wegen ihres engen Zusammenhanges mit der Haupttätigkeit und wegen ihrer untergeordneten Bedeutung gegenüber dieser Haupttätigkeit nach der Verkehrsauffassung in dieser gleichsam aufgeht“*.<sup>11</sup> Dabei sind im Sinne eines beweglichen Systems z.B. Geschäftsplan und -strategie, Ressourceneinsatz, Ertrag, Akquisition und Marketing etc. heranzuziehen.<sup>12</sup> Es ist darauf abzustellen, ob eine bestimmte Tätigkeit *„ihrer Natur nach selbständigen Charakter aufweist oder aber rein akzessorisch zu anderen [...] Tätigkeiten des Unternehmens ist“*.<sup>13</sup> Zu beachten ist in diesem Zusammenhang, dass dem Begriff der Haupttätigkeit ein gewerberechtlich geprägtes Verständnis zugrunde liegt und ein Unternehmen nicht nur eine Haupttätigkeit haben kann.<sup>14</sup>
- 6 Dienstleister in Bezug auf virtuelle Währungen ist, wer als natürliche oder juristische Person mit (Wohn)Sitz im Inland oder vom Inland aus eine Dienstleistung gemäß § 2 Z 22 FM-GwG in Bezug

<sup>8</sup> Bundesgesetz über die Sanierung und Abwicklung von Banken (BaSAG), BGBl. I Nr. 98/2014, in der geltenden Fassung.

<sup>9</sup> Bundesgesetz zur Schaffung einer Abbaueinheit (GSA), BGBl. I Nr. 51/2014, in der geltenden Fassung.

<sup>10</sup> VwGH 10.11.2017, Ro 2017/02/0023 mwN.

<sup>11</sup> BVwG 02.08.2017, W230 2150836-1 mwN.

<sup>12</sup> Dabei können u.a. auch der Außenauftritt, der Firmenname oder die auf der Homepage des Unternehmens beworbenen Tätigkeit für die Beurteilung herangezogen werden. Außerdem ist zu berücksichtigen, ob für die Ausübung der betroffenen Tätigkeit *„andere Gegenstände, andere Vermögenswerte, eine andere Organisation und Maßnahmen notwendig sind“* (BVwG 02.08.2017, W230 2150836-1).

<sup>13</sup> BVwG 02.08.2017, W230 2150836-1 mwN.

<sup>14</sup> IdS auch BVwG 02.08.2017, W230 2150836-1.

auf virtuelle Währungen gemäß § 2 Z 21 FM-GwG gewerbsmäßig für Dritte erbringt. Ebenso umfasst sind jene Dienstleister in Bezug auf virtuelle Währungen, die mit Sitz in einem anderen EU-Mitgliedsstaat oder Drittstaat eine Dienstleistung gemäß § 2 Z 22 FM-GwG aktiv im Inland anbieten oder erbringen.

- 7 Bei der Einschätzung des Risikos im Hinblick auf Geldwäscherei und Terrorismusfinanzierung sind durch die Verpflichteten sämtliche relevanten Risiken zu analysieren, um deren Auswirkungen auf ihr Unternehmen zu verstehen. Die Risikoanalyse bildet daher das Fundament für den risikoorientierten Ansatz bei den zu setzenden risikomitigierenden Maßnahmen.
- 8 Der risikoorientierte Ansatz ist kein „zero failure“-Ansatz. Es ist denkbar, dass Verpflichtete angemessene Maßnahmen der Risikoidentifizierung und -minimierung ergriffen haben und trotzdem für die Zwecke der Geldwäscherei und Terrorismusfinanzierung missbraucht werden.
- 9 Im Jahr 2012 wurden die Empfehlungen der Financial Action Task Force (FATF) – die internationalen Standards zur Prävention von Geldwäscherei und Terrorismusfinanzierung – einer grundlegenden Aktualisierung unterzogen. Eine der wichtigsten Änderungen ist die bedeutende Ausweitung des risikoorientierten Ansatzes, insbesondere im Hinblick auf die Präventionsmaßnahmen. Empfohlen die Standards 2003 noch den risikoorientierten Ansatz in bestimmten Bereichen der Geldwäscheprevention, so wird der risikoorientierte Ansatz in den Empfehlungen 2012 als essentielle Grundlage einer effektiven Geldwäscheprevention erörtert. Der risikoorientierte Ansatz ist nunmehr die umfassende Voraussetzung, die sich über den gesamten Umfang der Sorgfaltspflichten erstreckt. Dies erlaubt den Normunterworfenen einen selbstbestimmteren und somit flexibleren, im Hinblick auf die jeweiligen Risiken variablen Einsatz von Maßnahmen; Ressourcen können daher gezielter und effizienter eingesetzt werden.
- 10 Die Implementierung des risikoorientierten Ansatzes ist daher keinesfalls optional, sie ist die Voraussetzung für die effektive Umsetzung der Anforderungen des FM-GwG.
- 11 Das vorliegende Rundschreiben beinhaltet die Überlegungen der FMA im Hinblick auf das Fundament des risikoorientierten Ansatzes der Verpflichteten: die Risikoanalyse auf Unternehmens- sowie auf Einzelkundenebene. Die Informationen in diesem Rundschreiben sollen als Hilfestellung dienen, weiters stellt das Dokument die Rechtsansicht der FMA betreffend die Risikoanalyse der Verpflichteten dar.
- 12 Die Erstellung dieses Rundschreibens erfolgte unter Berücksichtigung der von der Europäischen Bankenaufsichtsbehörde (EBA) veröffentlichten Leitlinien nach Artikel 17 und Artikel 18 Absatz 4 der Richtlinie (EU) 2015/849 über Sorgfaltspflichten und die Faktoren, die Kredit- und Finanzinstitute bei der Bewertung des mit einzelnen Geschäftsbeziehungen und gelegentlichen Transaktionen verknüpften Risikos für Geldwäsche und Terrorismusfinanzierung berücksichtigen sollten („Die Leitlinien zu den Risikofaktoren für Geldwäsche und Terrorismusfinanzierung“), zur Aufhebung und Ersetzung der Leitlinien JC/2017/37, März 2021 (EBA/GL/2021/02). Leitlinien der EBA legen fest, was nach Ansicht der EBA angemessene Aufsichtspraktiken im Bereich der Prävention von Geldwäscherei und Terrorismusfinanzierung innerhalb des europäischen Finanzaufsichtssystems sind oder wie das Unionsrecht in einem bestimmten Bereich anzuwenden

ist. Gemäß Artikel 16 Absatz 3 der EBA-Verordnung<sup>15</sup> müssen die zuständigen Behörden und die Finanzinstitute alle erforderlichen Anstrengungen unternehmen, um den Leitlinien nachzukommen. Gemäß § 25 Abs. 3 FM-GwG hat die FMA Leitlinien und Empfehlungen und andere von der EBA beschlossene Maßnahmen anzuwenden.

- 13 Bei allen personenbezogenen Bezeichnungen gilt die gewählte Formulierung für beide Geschlechter.

---

<sup>15</sup> Verordnung (EU) Nr. 1093/2010.

## 2 NATIONALE RISIKOANALYSE

- 14 Gemäß § 3 Abs. 1 FM-GwG ist beim Bundesminister für Finanzen (BMF) ein Koordinierungsgremium zur Ermittlung, zur Bewertung, zum Verständnis und zur Minderung der im Inland bestehenden Risiken der Geldwäscherei und Terrorismusfinanzierung und aller Datenschutzprobleme in diesem Zusammenhang sowie zur Entwicklung von Maßnahmen und Strategien zur Verhinderung der Geldwäscherei und Terrorismusfinanzierung einzurichten. Das Koordinierungsgremium hat unter anderem eine nationale Risikoanalyse zu erstellen (§ 3 Abs. 2 FM-GwG). Die nationale Risikoanalyse dient vor allem der Verbesserung des Systems zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung und soll zu diesem Zweck unter anderem auch der umgehenden Versorgung der Verpflichteten mit angemessenen Informationen dienen, damit diese ihre eigene Bewertung des Risikos der Geldwäscherei und Terrorismusfinanzierung leichter vornehmen können (§ 3 Abs. 3 Z 6 FM-GwG).
- 15 Verpflichtete haben bei der Erstellung der Risikoanalyse auf Unternehmensebene gemäß § 4 Abs. 1 FM-GwG die Ergebnisse der nationalen Risikoanalyse (§ 3 FM-GwG) und des Berichts der Europäischen Kommission über die Risiken der Geldwäscherei und Terrorismusfinanzierung im Binnenmarkt gemäß Art. 6 Abs. 1 der 4. Geldwäsche-RL (Supranationale Risikoanalyse) zu berücksichtigen.

### 2.1 Einleitung

- 16 Für die Zwecke dieses Rundschreibens wird in den nachstehenden Ausführungen auf die Nationale Risikoanalyse der Geldwäscherei und Terrorismusfinanzierung Österreichs (Stand: 11.05.2021) Bezug genommen. Sie soll exemplarisch illustrieren, welche relevanten Erkenntnisse die Verpflichteten daraus gewinnen können, um sie in weiterer Folge in ihre eigene Risikoanalyse auf Unternehmensebene einfließen zu lassen.

### 2.2 Inhalt

- 17 Die Nationale Risikoanalyse ermittelt und bewertet einerseits „Bedrohungen und Bedrohungsfaktoren“, die sich von kriminellen Aktivitäten (z.B. Vortaten) und gewissen Phänomenen ableiten lassen. Andererseits werden potentielle „Schwachstellen“ des nationalen Systems der Prävention von Geldwäscherei und Terrorismusfinanzierung anhand von politischen, wirtschaftlichen, sozialen, technologischen und legislativen Faktoren ermittelt und bewertet und werden daraus u.a. Maßnahmen (Prioritäten und Strategien) abgeleitet, um die Geldwäscherei und Terrorismusfinanzierung wirksam zu bekämpfen. Die zu diesen Faktoren ermittelten Ergebnisse und Maßnahmen sind seitens der Verpflichteten – sofern für sie von Relevanz – entsprechend zu berücksichtigen. Die Nationale Risikoanalyse orientiert sich dabei zur Risikoeinschätzung an der Methodologie der Supranationalen Risikoanalyse (SNRA) – mit folgender Definition des Gesamtrisikos:

Gesamtrisiko = 40 % Bedrohung + 60 % Verletzbarkeit – risikomindernde Maßnahmen
---

## 2.3 Vortaten, Methoden, Bedrohungen und Risiken

- 18 In der Nationalen Risikoanalyse finden sich Aufzählungen und Analysen zu spezifischen Vortaten und Methoden der Geldwäscherei, Bedrohungen sowie Risiken iZm Geldwäscherei, Terrorismusfinanzierung und Proliferationsfinanzierung. Im Folgenden soll ein Überblick gegeben werden.<sup>16</sup>
- 19 So sind etwa folgende Vortaten zur Geldwäscherei die häufigsten:
- Betrugskriminalität
  - Erpressung
  - Suchtkriminalität
  - Organisierte Kriminalität
  - Menschenhandel und Schlepperei
- 20 Hervorgehoben werden sollen insbesondere folgende Bedrohungen im Rahmen der Geldwäscherei:
- Betrug und Schmuggel im Zollbereich (Gesamtrisiko: mittel)
  - Steuervortaten wie z.B. Abgabenhinterziehung und Schmuggel (Gesamtrisiko: mittel)
  - Betrug in Verbindung mit „Offshore“ (Gesamtrisiko: sehr hoch)
  - Virtuelle Währungen und Kryptoassets (Gesamtrisiko: sehr hoch)
- 21 Die häufigsten Methoden, die für Geldwäscherei genutzt werden, sind die Folgenden:
- Kryptowährungen
  - Money Mules<sup>17</sup>
  - Hawala
  - Urkundenfälschung
- 22 Im Zusammenhang mit Terrorismusfinanzierung sind folgende Bedrohungsszenarien hervorzuheben:
- Mittelaufbringung – Spenden
  - Überweisungen in Drittstaaten
- 23 Im Zusammenhang mit Proliferationsfinanzierung besteht ebenso ein Risiko für österreichische Institute. 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

---

<sup>16</sup> Für nähere Details und Ausführungen siehe Nationale Risikoanalyse S. 8 ff.

<sup>17</sup> Es handelt sich hierbei um sogenannte „Geldtransportesel“, die illegale Gelder weiterleiten.

wesentlichen proliferationsbezogenen Gefährdungen dar. 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 Teilbereichen 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.

- 24 Auch juristische Personen und Trusts können für die Zwecke von Geldwäscherei und Terrorismusfinanzierung missbraucht werden. In der Nationalen Risikoanalyse findet sich in diesem Zusammenhang eine detaillierte Analyse der WiEReG-Registerbehörde zu den einzelnen Gesellschaftsformen und dem korrespondierenden Risiko.

## 2.4 Ausführungen und Ergebnisse zum Finanzmarkt

- 25 Bei der Beurteilung der einzelnen Sub-Sektoren (Kreditinstitute, Versicherungsunternehmen etc.) des Finanzsektors in der Nationalen Risikoanalyse handelt es sich um keine absolute Einschätzung des konkreten Geldwäscherei- und Terrorismusfinanzierungs-Risikos der einzelnen (österreichischen) Sub-Sektoren. Die jeweilige Beurteilung bezieht sich vielmehr auf die relative Risikogeneignetheit eines Sub-Sektors im Vergleich zu anderen Branchen anhand objektiverer, struktureller Risikokriterien. So ist z.B. das abstrakte Geldwäscherei- und Terrorismusfinanzierungs-Risiko von österreichischen Kreditinstituten jedenfalls höher einzuschätzen als jenes von österreichischen Versicherungsunternehmen. Dies bedeutet jedoch nicht, dass der österreichische Bankensektor deshalb in concreto einem hohen Risiko unterliegt oder gar eine potentielle Schwachstelle darstellt.
- 26 Im Folgenden werden im Überblick die Ergebnisse der einzelnen Sub-Sektoren des Finanzsektors dargestellt<sup>18</sup>:

<b>Subsektor</b>	<b>GW-Risiko</b>	<b>TF-Risiko</b>
Guthaben bei Kredit- und Finanzinstituten (KI/FI)	hoch	hoch
Kapitalanlagegesellschaften (KAG) – Immobilien-Kapitalanlagegesellschaften (Immo-KAG) – Alternative Investmentfonds Manager (AIFM)	mittel	niedrig
Wertpapierfirmen (WPF) und Wertpapierdienstleistungsunternehmen (WPDLU)	mittel	niedrig
Private Banking-Vermögensverwaltung	mittel bis hoch	niedrig

<sup>18</sup> Für Details zur Sektoranalyse Finanzsektor bitte siehe die Nationale Risikoanalyse ab Seite 42ff.

Crowdfunding	mittel	mittel für den reglementierten Bereich; mittel bis hoch für den nicht-reglementierten Bereich
Wechselstuben	mittel	mittel
Elektronisches Geld (E-Geld)	mittel	mittel
Zahlungsdienste	hoch	hoch
Virtuelle Währungen	hoch	hoch
„Back-To-Back“-Geschäftsmodelle (Treuhandkredite)	hoch	niedrig
Lebensversicherung	niedrig	niedrig
Safe-Vermietung	mittel	niedrig
Geschäftskredite	niedrig	niedrig
Konsumenten- bzw. Kleinkredite	mittel	mittel bis hoch
Hypothekarkredite	mittel	niedrig

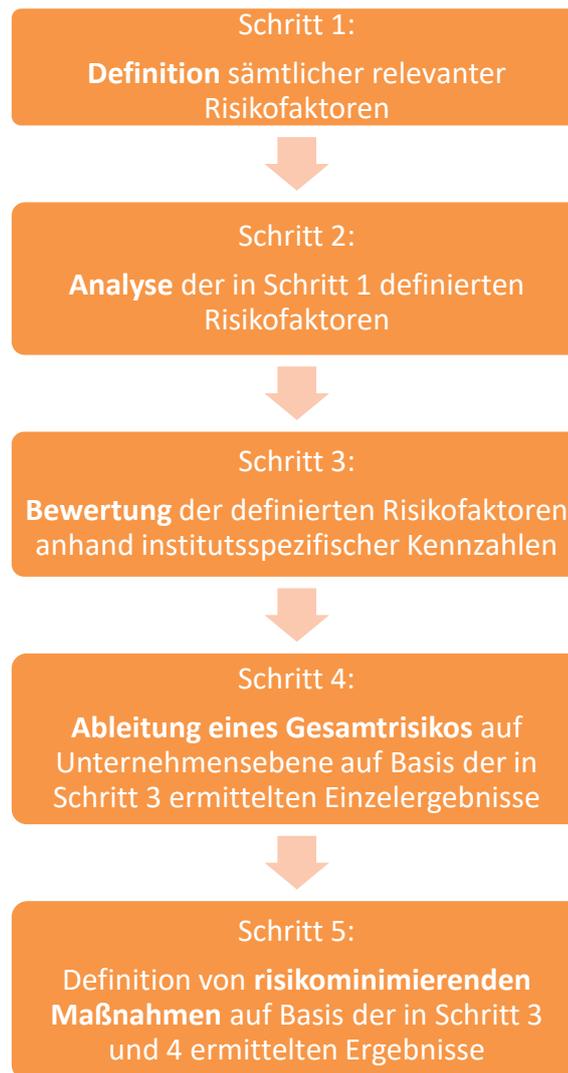
## 3 RISIKOANALYSE AUF UNTERNEHMENSEBENE

### 3.1 Allgemeines und Methodik

- 27 Die Verpflichteten haben gemäß § 4 FM-GwG die potentiellen Risiken der Geldwäscherei und Terrorismusfinanzierung, denen ihr Unternehmen ausgesetzt ist, zu ermitteln, zu bewerten und zu mitigieren. Die entsprechenden Ermittlungs- und Bewertungsschritte haben in einem angemessenen Verhältnis zu Art und Größe des Verpflichteten zu stehen und sind inkl. ihrem Ergebnis nachvollziehbar zu dokumentieren. Diese Aufzeichnungen sind in regelmäßigen Abständen – zumindest jährlich – zu aktualisieren. Auf Anfrage ist die Risikobewertung der FMA in einem allgemein gebräuchlichen elektronischen Format zur Verfügung zu stellen.
- 28 Vereinfacht dargestellt ist im Rahmen der Risikoanalyse auf Unternehmensebene u.a. auf folgende Fragen einzugehen:
- Welche Risikofaktoren sind im Hinblick auf die Geschäftsstrategie und die institutsspezifische Situation des Verpflichteten relevant?
  - Welches Risiko stellen die identifizierten Risikofaktoren für den Verpflichteten konkret dar?
  - Welche Maßnahmen können auf Unternehmensebene gesetzt werden, um das Risiko entsprechend zu mitigieren?

### 3.2 Praktischer Leitfaden zur Erstellung

- 29 Einleitend sind hinsichtlich der institutsspezifischen Situation etwa allgemeine Unternehmenskennzahlen, Geschäftsstrategie (z.B. Geschäftspolitik und -bereiche) sowie Geschäftsumfeld und Zielmarkt darzustellen. Dabei ist beispielhaft auf die nachstehenden Punkte einzugehen:
- Wie ist das Institut organisiert (Hauptsitz, Bilanzsumme, Mitarbeiter, Vorstand, Aufsichtsrat, wesentliche Beteiligungen)?
  - In welchen Bereichen bestehen Auslagerungen?
  - Wie gestalten sich das Geschäftsumfeld und der Zielmarkt (z.B. Regionsprofil, Profil potentieller Kunden)?
  - Welchen Einfluss haben das nationale und regulatorische Umfeld, die Entwicklung der Kriminalitätslage bzw. mögliche aktuelle Phänomene?
  - Wie sind Geschäftspolitik und -bereiche (Kerngeschäft, etc.) ausgestaltet?
  - Welche Vertriebskanäle (z.B. über qualifizierte Dritte oder Vermittler) bestehen?
  - Inwiefern kommen neue Technologien (etwa im Zusammenhang mit der Kundenidentifizierung) zum Einsatz?
- 30 Die praktische Vorgehensweise der Verpflichteten bei der Erstellung einer entsprechenden Risikoanalyse auf Unternehmensebene lässt sich in fünf Arbeitsschritte unterteilen:



### 3.2.1 Schritt 1: Definition sämtlicher relevanter Risikofaktoren

31 In einem ersten Schritt ist zu definieren, welche Risikofaktoren für die Verpflichteten im Hinblick auf die konkrete institutsspezifische Situation bzw. auf die Geschäftsstrategie relevant sind. Hierfür sind auch insb. die sog. EBA ML/TF RF GI zu berücksichtigen.<sup>19</sup> Ebenso gibt auch die alle zwei Jahre aktualisierte Supranationale Risikoanalyse<sup>20</sup> der EU wertvollen Input für die Definition sowie Analyse relevanter Risikofaktoren.

32 Basierend auf der dargelegten institutsspezifischen Situation sind sämtliche für den Verpflichteten relevanten Risikofaktoren zu erheben. Einzugehen ist dabei zumindest auf jene Risikofaktoren, die demonstrativ in § 4 Abs. 1 FM-GwG aufgezählt werden, und zwar in Bezug auf

<sup>19</sup> EBA Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849; [https://www.eba.europa.eu/sites/default/documents/files/document\\_library/Publications/Guidelines/2021/963637/Final%20Report%20on%20Guidelines%20on%20revised%20ML%20TF%20Risk%20Factors.pdf](https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/963637/Final%20Report%20on%20Guidelines%20on%20revised%20ML%20TF%20Risk%20Factors.pdf).

<sup>20</sup> Supranational risk assessment of the money laundering and terrorist financing risks affecting the Union (Stand 24. Juli 2019); [https://ec.europa.eu/info/files/supranational-risk-assessment-money-laundering-and-terrorist-financing-risks-affecting-union\\_en](https://ec.europa.eu/info/files/supranational-risk-assessment-money-laundering-and-terrorist-financing-risks-affecting-union_en).

- a. Kunden,
  - b. Länder oder geografische Gebiete,
  - c. Produkte,
  - d. Dienstleistungen,
  - e. Transaktionen,
  - f. Vertriebskanäle sowie
  - g. sonstige neue oder sich entwickelnde Technologien.
- 33 Grundsätzlich hat der Fokus bei der Definition dieser Risikofaktoren – wie auch bei der weiteren Bewertung und Mitigierung – auf der konkret durchgeführten Tätigkeit des Verpflichteten zu liegen. Entsprechend kurz kann – in einem angemessenen Verhältnis zu Art und Größe der Verpflichteten – die Risikoanalyse ausfallen, wenn lediglich ein sehr eingeschränktes Geschäftsfeld vorliegt.

### 3.2.2 Schritt 2: Analyse der definierten Risikofaktoren

- 34 In einem zweiten Schritt sind die ermittelten Risikofaktoren zu analysieren. Das bedeutet, dass (zumindest) sämtliche in Rz 32 aufgezählten Risikofaktoren sowie die jeweils relevanten Subkriterien bzw. ihre Bedeutung für die Bewertung des jeweiligen Risikos sowie ihre grundsätzliche Auswirkung auf das Unternehmensrisiko zu erfassen sind.
- 35 Für die Beurteilung des Länderrisikos sind einzelne Länder, z.B. nach dem Entwicklungsstand und der Transparenz ihres Rechtssystems, des Maßes an Rechtssicherheit, der Stabilität ihrer wirtschaftlichen und politischen Verhältnisse, der Kriminalitätsrate, der Stabilität ihres Finanzmarktes, dem Korruptionsgrad sowie den landesüblichen Firmenregistern sowie Offenlegungs- und Transparenzerfordernissen zu beurteilen. Dabei können etwa verschiedene Länderlisten herangezogen werden, vgl. Rz 76 und Rz 93f. Aufgrund dieser Beurteilung können Länder z.B. in EU-Mitgliedstaaten, gleichwertige Drittländer, Drittländer mit hohem Risiko gemäß § 2 Z 16 FM-GwG, von Sanktionen betroffene Staaten, Offshore-Länder, Länder mit hoher Korruption kategorisiert werden. Offshore-Ländern oder Ländern mit ausgeprägter Korruption ist z.B. ein hohes Risiko zuzuweisen.
- 36 Das Produktrisiko hängt u.a. von dem Missbrauchspotential ab, das mit dem angebotenen Produkt im Hinblick auf Geldwäscherei bzw. Terrorismusfinanzierung verbunden ist. Abzustellen ist dabei auf den Grad der Anonymität, z.B. bei gewissen virtuellen Währungen, den Bargeldcharakter, die Liquidität, die Vertriebskanäle sowie die Komplexität der Produkte. Eine anonyme Nutzungsmöglichkeit (z.B. Prepaidkarten, etc.), eine erhöhte Bargeldintensität, eine jederzeitige Verfügbarkeit von Liquidität sowie komplexe Produkte (z.B. Back-to-back-Treuhandgeschäftsmodell, Derivate, strukturierte oder gehebelte Produkte, etc.) erhöhen im Hinblick auf die damit verbundenen mangelnden oder erschwerten Kontrollmöglichkeiten das Risiko, für die Zwecke der Geldwäscherei oder Terrorismusfinanzierung missbraucht zu werden.
- 37 Hinsichtlich des Transaktionsrisikos erfolgt eine Zuordnung anhand der Nachvollziehbarkeit bzw. der Möglichkeit, die Nachvollziehbarkeit der Transaktionen zu unterbrechen („paper trail“). So wirken etwa Transaktionen über Durchlaufkonten, gelegentliche Transaktionen, Transaktionen

iZm Offshore-Konstrukten oder ein hoher Anteil des Auslandszahlungsverkehrs iZm Ländern mit erhöhtem Risiko aufgrund der Verschleierungsmöglichkeit bzw. der möglichen Anonymität risikoe erhöhend. Ebenso sind Bartransaktionen und grenzüberschreitende Transaktionen, insbesondere sofern involvierte Institute keine gleichwertigen Sorgfaltspflichten einzuhalten haben, als risikoe erhöhend zu erachten.

- 38 Das Kundenrisiko ist u.a. anhand der Kundeneigenschaften, wie z.B. natürliche oder juristische Person inklusive des wirtschaftlichen Eigentümers, Wohnsitz/Sitz, Rechtsform, Private-Banking-Kunde, PEP sowie Branche des Kunden (Bargeldintensität, Transaktionsintensität, Auslandsbezug) zu beurteilen. Dabei ist etwa komplexen Eigentums- und Kontrollstrukturen, die eine Möglichkeit zur Anonymisierung bzw. Verschleierung der Eigentumsstruktur und/oder der Mittelherkunft begünstigen, oder bestimmten Branchen, die ein hohes Maß an Bargeld bzw. Transaktionen aufweisen, hohes Risiko zuzuweisen.
- 39 Das Risiko in Bezug auf Vertriebskanäle ist u.a. unter Berücksichtigung der Intensität des Kundenkontaktes bei Erfüllung der Sorgfaltspflichten zur Prävention von Geldwäsche und Terrorismusfinanzierung zu beurteilen. So ist Vertriebskanälen, im Rahmen derer etwa Vermittler zum Einsatz kommen, z.B. ein höheres Risiko zuzuweisen (vgl. auch Rz 65 ff sowie Rz 77 ff).
- 40 Zu beurteilen ist weiters das Risiko in Bezug auf neue oder sich entwickelnde Technologien, wobei – entsprechend der FATF-Empfehlung 15 – sowohl Risiken, die sich aus der Entwicklung neuer Produkte oder neuer Geschäftspraktiken ergeben, als auch solche, die aus dem Gebrauch neuer Technologien resultieren, zu berücksichtigen sind. Das sich aus neuen oder sich entwickelnden Technologien ergebende Risiko ist seitens der Verpflichteten jedenfalls bereits vor der Einführung der jeweiligen Produkte oder Geschäftspraktiken zu evaluieren.
- 41 Weitere Faktoren, die in diesem Zusammenhang hinsichtlich des Risikogehaltes aussagekräftig sein können, sind etwa auch rechtliche Anforderungen, Anforderungen der Aufsicht, Erkenntnisse aus Verdachtsfällen oder aktuelle Ereignisse.
- 42 Seitens der Verpflichteten ist die Analyse der Risikofaktoren und ihrer Subkriterien nach den dargelegten Grundsätzen im Rahmen der Risikoanalyse zu verschriftlichen und z.B. in folgender Form festzuhalten: „*Geschäftsbeziehungen mit Offshore-Bezug sind als hohes Risiko anzusehen, weil..., Das Risiko im Hinblick auf Bartransaktionen ist als hoch anzusehen, weil...;*“.

### 3.2.3 Schritt 3: Bewertung der definierten Risikofaktoren

- 43 Anknüpfend an die Definition und die Analyse der relevanten Risikofaktoren hat als Schritt 3 eine Bewertung der Risikofaktoren unter Berücksichtigung institutsspezifischer Kennzahlen zu erfolgen. In der Folge sind die einzelnen Risikofaktoren durch entsprechendes institutseigenes Zahlen- und Datenmaterial zu illustrieren bzw. in ein Verhältnis zu bringen und – als Zwischenergebnis – zu bewerten. So hat seitens der Verpflichteten eine Bewertung der einzelnen ermittelten Teilrisiken unter Berücksichtigung ihrer institutsspezifischen Kennzahlen zu erfolgen.
- 44 Eine zusammenfassende Bewertung der einzelnen Faktoren ohne vorherige detaillierte Analyse und Hinterlegung mit institutsspezifischen Kennzahlen ist jedenfalls nicht ausreichend. Vielmehr muss aus der Bewertung klar ersichtlich sein, wie viele – beispielsweise – Geschäftsbeziehungen

zu Kunden, die gleichzeitig auch die PEP-Eigenschaft erfüllen und in welcher Relation dieser Risikofaktor zum Unternehmen bzw. zur Tätigkeit des Unternehmens steht. Anders formuliert: Es wirkt sich anders auf die Risikobewertung aus, ob beispielsweise 0,25 % oder 10 % des Gesamtkundenbestandes einen Offshore-Bezug aufweisen. Dieser Umstand muss aus der seitens des Verpflichteten vorgenommenen Bewertung ableit- und überprüfbar sein.

- 45 Eine nachvollziehbare Verschriftlichung der Bewertung des Transaktionsrisikos könnte beispielsweise folgende Form haben: *„Rund 0,5 % des abgewickelten Transaktionsvolumens (dies entspricht EUR xxx) weisen einen Auslandsbezug in Länder innerhalb des EWR auf. Transaktionen in Drittländer stellen im vergangenen Jahr lediglich etwa 0,01 % des abgewickelten Transaktionsvolumens (dies entspricht EUR xxx) dar. Der Anteil von Bartransaktionen, deren Risiko grundsätzlich als hoch bewertet wurde, entspricht rund 0,2 % (dies entspricht EUR xxx) des abgewickelten Transaktionsvolumens, und spielt somit eine untergeordnete Rolle. Das transaktionsbezogene Risiko wird sohin als gering erachtet.“*
- 46 Das Ergebnis der einzelnen Risikofaktoren muss letztlich plausibel sein: Ergibt etwa die Analyse des Kundenrisikos, dass ein hoher Prozentsatz des Gesamtkundenbestandes den Wohnsitz/Sitz in Ländern mit erhöhtem Risiko unterhält und ein weiterer beträchtlicher Teil der Geschäftsbeziehungen einen PEP-Bezug aufweist, wird auch das Kundenrisiko als hoch zu bewerten sein.

#### 3.2.4 Schritt 4: Ableitung eines Gesamtrisikos auf Unternehmensebene

- 47 Als Schritt 4 ist aus den Teilergebnissen ein (schlüssiges) Gesamtrisiko abzuleiten. Dies bedeutet, wenn z.B. das Länderrisiko als gering, das Produktrisiko als mittel, das Transaktionsrisiko als hoch und das Kundenrisiko als mittel eingestuft wurde, daraus ein entsprechendes Gesamtrisiko auf Unternehmensebene für Zwecke der Geldwäscherei und der Terrorismusfinanzierung missbraucht zu werden, abzuleiten ist, in welchem sich die ermittelten Werte widerspiegeln.

#### 3.2.5 Schritt 5: Risikominimierende Maßnahmen

- 48 Letztlich ist als Schritt 5 zu definieren bzw. abzubilden, welche risikoorientierten Maßnahmen auf Unternehmensebene gesetzt werden können, um das Risiko entsprechend zu minimieren. Davon umfasst sind z.B.:
- angemessene Strategien und Verfahren zur Einhaltung der Sorgfaltspflichten inkl. entsprechender Verschriftlichung in Dienstanweisungen, Arbeitsbehelfen (wie z.B. Checklisten, Kundenannahmeprozessen, Formularen o.ä.);
  - die Ausstattung der Funktion des Geldwäschebeauftragten (GWB) mit entsprechenden (ausreichenden) Ressourcen und Kompetenzen (z.B. Einbeziehung des GWB bei Begründung der Geschäftsbeziehung zu Kunden mit hohem Risiko);
  - die zumindest jährliche Aktualisierung der Risikoanalyse;
  - die Erhebung erforderlicher Daten inkl. Einbindung anderer Abteilungen sowie die Sicherung der Datenqualität (auch im Hinblick auf den Detaillierungsgrad der Daten);
  - regelmäßige Mitarbeiterschulungen und Sensibilisierung betreffend mögliche Risikosituationen;

- f. den Einsatz von IT-Systemen zur Prävention von Geldwäscherei und Terrorismusfinanzierung;
- g. Durchführung von Kontrollen inkl. Verschriftlichung im Rahmen eines Kontrollplanes;
- h. Dokumentation der Ergebnisse der durchgeführten Maßnahmen.

## 4 RISIKOANALYSE AUF EINZELKUNDENEBENE

- 49 Gemäß § 6 Abs. 5 FM-GwG können die Verpflichteten den Umfang der in § 6 Abs. 1 bis 3 FM-GwG genannten Sorgfaltspflichten auf risikoorientierter Grundlage bestimmen. Bei der Bewertung der Risiken von Geldwäscherei und Terrorismusfinanzierung sind zumindest die in Anlage I des FM-GwG aufgeführten Variablen zu berücksichtigen. Als Ergebnis dieser Bewertung ist jeder Kunde in eine Risikoklasse einzustufen. Die Verpflichteten müssen der FMA gegenüber nachweisen können, dass die von ihnen getroffenen Maßnahmen angesichts der ermittelten Risiken von Geldwäscherei und Terrorismusfinanzierung angemessen sind.
- 50 Um als Verpflichtete sicherstellen zu können, dass ein allfälliger Hochrisikokunde als solcher erkannt wird, hat über die Bewertung der Risikovariablen der Anlage I hinaus weiters die Berücksichtigung von zumindest der in der Anlage III des FM-GwG angeführten Risikovariablen zu erfolgen, vgl. Rz 77. Im Hinblick auf Geschäftsbeziehungen, welche ein hohes Risiko im Hinblick auf Geldwäscherei oder Terrorismusfinanzierung darstellen und einer entsprechenden verstärkten Überwachung bedürfen, ist daher die ausschließliche Berücksichtigung der in Anlage I genannten Risikovariablen bei der Risikoklassifizierung als nicht ausreichend zu erachten.
- 51 Damit seitens eines Verpflichteten die Feststellung möglich ist, dass auf einen Kunden vereinfachte Sorgfaltspflichten anwendbar sind, sind darüber hinaus die Risikovariablen der Anlage II des FM-GwG in die Risikoanalyse auf Kundenebene miteinzubeziehen.

### 4.1 Identifizierung und Bewertung der Risiken von Geldwäscherei und Terrorismusfinanzierung

#### 4.1.1 Erstellung des Risikoprofils

- 52 Um das Risiko, welches eine Geschäftsbeziehung im Hinblick auf Geldwäscherei und Terrorismusfinanzierung darstellt, beurteilen zu können, müssen Verpflichtete über ausreichend Wissen über den Kunden sowie das zu erwartende Kunden- und Transaktionsverhalten verfügen.<sup>21</sup> Die Einholung ausreichender Informationen über den Kunden wird durch die Implementierung umfassender Prozesse zur Einhaltung der gesetzlich normierten Sorgfaltspflichten sichergestellt. Nach erfolgtem „Customer due diligence Prozess“ (CDD) verfügen Verpflichtete über ausreichende Kenntnis im Hinblick auf die Identität von Kunden, welcher Tätigkeit Kunden nachgehen und aus welchem Grund sie sich für den Verpflichteten entschieden haben.
- 53 Die ersten Schritte, die durch Verpflichtete im Rahmen der CDD gesetzt werden, ermöglichen das Risiko der Geldwäscherei und Terrorismusfinanzierung, welches von der Geschäftsbeziehung ausgeht, zu bewerten und folglich zu entscheiden, in welchem Umfang Sorgfaltspflichten anzuwenden sind.

---

<sup>21</sup> Für zu berücksichtigende Kriterien siehe auch die Ausführungen zu den EBA ML/TF Risk Factor Guidelines sowie der Supranationale Risikoanalyse der EU unter Punkt 3.2.1.

- 54 Basierend auf den im Rahmen der CDD eingeholten Know-Your-Customer-Informationen (KYC) sind Verpflichtete in der Lage, ein Risikoprofil des Kunden zu erstellen. Dieses Risikoprofil unterstützt die Verpflichteten bei der Entscheidung, ob eine Geschäftsbeziehung begründet bzw. fortgeführt oder beendet werden soll sowie in welchem Umfang Maßnahmen zu setzen sind.
- 55 Die Sorgfaltspflichten gemäß § 6 FM-GwG sind in jedem Fall einzuhalten. In welchem Ausmaß diese angewendet werden, hängt vom Risiko der jeweiligen Geschäftsbeziehung ab, vgl. Rz 54. Dies bedeutet, dass die Anforderung an Art und Umfang von Informationen, welche durch Verpflichtete einzuholen und in welchem Ausmaß diese zu überprüfen sind, mit dem Risiko, das mit einer Geschäftsbeziehung verbunden ist, steigt. In weiterer Folge bedeutet dies, dass das Ausmaß der Anwendung der Sorgfaltspflichten gemindert werden kann, wenn das mit der Geschäftsbeziehung verbundene Risiko als niedrig zu erachten ist.
- 56 Um sicherstellen zu können, dass das Ausmaß der Anwendung der Sorgfaltspflichten angemessen ist, sind Risikoprofile zu Beginn einer Geschäftsbeziehung zu erstellen und periodisch bzw. jedenfalls anlassbezogen zu aktualisieren.

#### 4.1.2 Anlage I

- 57 Bei der Bewertung der Risiken von Geldwäscherei und Terrorismusfinanzierung sind die in Anlage I des FM-GwG aufgeführten Variablen zu berücksichtigen, vgl. Rz 49.

##### 4.1.2.1 Zweck eines Kontos oder einer Geschäftsbeziehung

- 58 Das Verständnis über Zweck und Art der Geschäftsbeziehung ist ein wesentlicher und für die Risikoklassifizierung eines Kunden erforderlicher Faktor. Je nach Kunden und durch diesen in Anspruch genommenen Dienstleistungen sind die Anforderungen an die Einholung und Dokumentation von Zweck und Art der Geschäftsbeziehung durch den Verpflichteten unterschiedlich.
- 59 Je komplexer sich die Geschäftsbeziehung gestaltet, umso höher sind die Anforderungen an die Einholung und die schriftliche Dokumentation von Zweck und Art der Geschäftsbeziehung. Weist ein Kunde z.B. keinen (geographischen) Bezug zum Verpflichteten auf, so wäre zu dokumentieren, aus welchem Grund der Kunde bei einem bestimmten Verpflichteten Dienstleistungen in Anspruch nehmen möchte. Des Weiteren sollten die Verpflichteten nach erfolgten Kundengesprächen u.a. folgende Fragen beantworten können und hierüber eine schriftliche Dokumentation führen:
- Handelt es sich bei dem Kunden um einen Unternehmer, welcher Geschäftszweck wird durch das Unternehmen verfolgt?
  - Aus welchem Grund wird gerade diese Dienstleistung dieses Institutes in Anspruch genommen?
  - Ist der Hintergrund des Kunden und des wirtschaftlichen Eigentümers konsistent mit dem Wissen des Verpflichteten über frühere, aktuelle oder geplante geschäftliche Aktivitäten, Umsatz, Herkunft der Mittel des Kunden.
  - Für den Fall, dass der Kunde keinen geographischen Bezug zum Verpflichteten aufweist: Könnten die Bedürfnisse des Kunden andernorts besser bedient werden? Gibt es

nachvollziehbare wirtschaftliche oder rechtliche Gründe, dass der Kunde um bestimmte finanzielle Dienstleistungen ersucht?

#### 4.1.2.2 Höhe der von einem Kunden eingezahlten Vermögenswerte oder Umfang der ausgeführten Transaktionen

- 60 Die Beurteilung des Risikos der Höhe der von einem Kunden eingezahlten Vermögenswerte bzw. Umfang der ausgeführten Transaktionen kann grundsätzlich nur im Rahmen einer Gesamtbetrachtung des Kunden im Zusammenhang mit weiteren Risikofaktoren erfolgen: Transaktionen, welche für einen Kunden besonders hoch erscheinen mögen, können z.B. für Unternehmens- oder besonders vermögende Kunden alltäglich oder nicht von Besonderheit sein. Es ist daher im Sinne des risikoorientierten Ansatzes nicht zweckmäßig, einen allgemeinen Schwellenwert für eine „hohe“ Transaktion zu definieren, der für alle Kunden eines Verpflichteten angewendet werden kann. Vielmehr bedarf es einer differenzierten Betrachtung von Kundenart (z.B. Corporate-Kunde, KMU, Privatkunde, institutioneller Kunde), Zweck und Art der Geschäftsbeziehung, Geschäftstätigkeit des Kunden, Herkunft des Vermögens/der Mittel, etc.
- 61 Um feststellen zu können, ab welchem Schwellenwert es sich bei bestimmten Kunden um eine außergewöhnlich hohe Transaktion handelt, ist es z.B. möglich, Vergleiche von Peer-Groups in dem beaufsichtigten Institut vorzunehmen und so zu ermitteln, in welcher Höhe Transaktionen bei bestimmten Kunden, Branchen, etc., zu erwarten sind.
- 62 Vermögenswerte in ungewöhnlicher Höhe oder eine ungewöhnlich große Anzahl von Transaktionen im Vergleich zu jenen, die von Kunden mit ähnlichem Profil erwartet werden können, deuten auf erhöhtes Risiko hin.
- 63 Der Risikofaktor „Höhe der von einem Kunden eingezahlten Vermögenswerte oder Umfang der ausgeführten Transaktionen“ ist des Weiteren im Hinblick auf den sog. Geschäftszweig „Private Banking“ bzw. „Wealth Management“ besonders relevant. Aufgrund der Transaktionen, welche häufiger große Volumina umfassen, sowie aufgrund der großen Vermögen, die im Rahmen des „Wealth Management“ verwaltet werden, sind Verpflichtete, welche Vermögensverwaltung bzw. Private Banking anbieten, einem erhöhten Risiko ausgesetzt, von Kunden für die Verschleierung der Herkunft von Vermögenswerten missbraucht zu werden.

#### 4.1.2.3 Regelmäßigkeit oder Dauer der Geschäftsbeziehung

- 64 Langjährige Geschäftsbeziehungen, im Rahmen derer es regelmäßig zu Kundenkontakten kommt, stellen möglicherweise ein geringeres Risiko im Hinblick auf Geldwäscherei dar. Dies kann z.B. auf die Erfahrungswerte des Verpflichteten aus der Geschäftsbeziehung mit dem Kunden (keine Auffälligkeiten im Transaktionsverhalten, keine Änderung von maßgeblichen Umständen, etc.) zurückgeführt werden.

### 4.1.3 Anlage II

- 65 Soll im Hinblick auf eine Geschäftsbeziehung die Anwendung von vereinfachten Sorgfaltspflichten erfolgen, so ist es erforderlich, über die Risikofaktoren der Anlage I hinausgehend die Risikovariablen der Anlage II in die Risikoklassifizierung miteinzubeziehen: Gemäß § 8 Abs. 1 FM-

GWG können Verpflichtete vereinfachte Sorgfaltspflichten gegenüber Kunden anwenden, wenn diese aufgrund ihrer Risikoanalyse festgestellt haben, dass in bestimmten Bereichen nur ein geringes Risiko der Geldwäscherei oder Terrorismusfinanzierung besteht. Hierbei sind die Risiken für bestimmte Arten von Kunden, geografische Gebiete und für bestimmte Produkte, Dienstleistungen, Transaktionen oder Vertriebskanäle zu bewerten und zumindest die in Anlage II dargelegten Faktoren für ein potenziell geringes Risiko zu berücksichtigen.

#### 4.1.3.1 Risikofaktoren bezüglich Kunden

##### 4.1.3.1.1 Anlage II Z 1 lit. a

66 Bei börsennotierten Gesellschaften handelt es sich um

- a. solche Gesellschaften, deren Wertpapiere zum Handel auf einem geregelten Markt in einem oder mehreren Mitgliedstaaten zugelassen sind, oder
- b. börsennotierte Gesellschaften aus Drittländern, die gemäß einer auf Basis der Verordnungsermächtigung gemäß § 122 Abs. 10 Börsegesetz 2018 (BörseG 2018<sup>22</sup>) durch die FMA zu erlassenden Verordnung Offenlegungsanforderungen unterliegen, die dem Unionsrecht entsprechen oder mit diesem vergleichbar sind.

##### 4.1.3.1.2 Anlage II Z 1 lit. b

67 Im Rahmen der öffentlichen Verwaltung werden von den entsprechenden Organen die staatlichen Aufgaben besorgt. Dies ist in einem weiten Sinn zu verstehen und umfasst sowohl die Vollziehung durch Organe der Gerichtsbarkeit als auch die Vollziehung durch Organe der Verwaltung (im engeren Sinn). In beiden Fällen sind sowohl Handlungen im Bereich der Hoheits- als auch der Privatwirtschaftsverwaltung der öffentlichen Verwaltung zuzuordnen. In welcher Form die jeweiligen Einrichtungen dabei organisiert sind, ist gegenständlich nicht von Bedeutung. Vom Begriff der öffentlichen Verwaltung sind daher alle Arten von juristischen Personen des öffentlichen Rechts (Körperschaften [Gebiets- und Personalkörperschaften], Anstalten, Fonds/Stiftungen) als auch privatrechtlich organisierte juristische Personen, die hauptsächlich mit hoheitlichen Befugnissen ausgestattet sind (z.B. Austro Control GmbH, RTR GmbH), umfasst.

68 Darüber hinaus sind auch mit Rechtspersönlichkeit ausgestattete Organe und Einrichtungen der Europäischen Union vom gegenständlichen Begriff der öffentlichen Verwaltung erfasst. Solche Organe und Einrichtungen können sich zum einen direkt aus dem EUV/AEUV ergeben bzw. ist die Errichtung von solchen Einrichtungen direkt in den Verträgen vorgesehen. Andererseits können derartige Einrichtungen auch von den Organen der EU selbst errichtet werden (diese werden dann meist als „Agenturen“ bezeichnet).<sup>23</sup>

69 Für den Begriff des öffentlichen Unternehmens kann auf § 2 Z 6 lit. g FM-GwG zurückgegriffen werden. Demnach umfasst dies in Österreich insbesondere Unternehmen, bei denen der Bund oder ein Land mit mindestens 50 v.H. des Stamm-, Grund- oder Eigenkapitals beteiligt ist oder die der Bund oder ein Land alleine betreibt oder die der Bund oder ein Land durch finanzielle oder sonstige wirtschaftliche oder organisatorische Maßnahmen tatsächlich beherrscht. Die

<sup>22</sup> Börsegesetz 2018 (BörseG 2018), BGBl. I Nr. 107/2017, in der geltenden Fassung.

<sup>23</sup> Unter [https://europa.eu/european-union/about-eu/agencies\\_de](https://europa.eu/european-union/about-eu/agencies_de) kann nach solchen Agenturen und sonstigen Einrichtungen gesucht werden.

Einschränkung auf Landesunternehmen mit einem jährlichen Gesamtumsatz von mehr als 1 Mio. Euro ist im gegenständlichen Fall nicht relevant.

#### 4.1.3.1.3 Anlage II Z 1 lit. c

70 Zu Kunden mit Wohnsitz in geografischen Gebieten mit geringem Risiko gemäß Z 3 der Anlage II, siehe Rz 76.

#### 4.1.3.2 Risikofaktoren bezüglich Produkte, Dienstleistungen, Transaktionen oder Vertriebskanäle

##### 4.1.3.2.1 Anlage II Z 2 lit. a - c

71 Betreffend Z 2 lit a bis c der Anlage II kann auf § 2 Abs. 1 Z 1 bis 3 der Lebensversicherungs-Sorgfaltspflichtenverordnung (LV-SoV) verwiesen werden: § 2 Abs. 1 der LV-SoV beinhaltet eine Aufzählung jener Arten von Versicherungsverträgen, auf die vereinfachte Sorgfaltspflichten angewendet werden können. Dies gilt sowohl in Bezug auf die Kunden des Versicherungsunternehmens selbst (§ 2 Z 15 FM-GwG) als auch in Bezug auf die Begünstigten von solchen Versicherungsverträgen (§ 7 Abs. 4 FM-GwG). Hinsichtlich der in § 2 Abs. 1 Z 1 bis 3 der LV-SoV aufgeführten sog. Bagatellverträge soll die Rechtslage, wie sie aufgrund des § 130 Abs. 1 Z 2 lit. a und b VAG 2016 bis zum 31.12.2016 bestand, fortgeführt werden.<sup>24</sup>

Als sog. Bagatellverträge sind gemäß § 2 Abs. 1 Z 1 bis 3 LV-SoV folgende Versicherungsverträge zu erachten:

- a. Lebensversicherungsverträge, bei denen die Höhe der im Laufe des Jahres zu zahlenden Prämien 1 200 Euro nicht übersteigt;
- b. Lebensversicherungsverträge, bei denen bei Zahlung einer einmaligen Prämie diese nicht mehr als 2 500 Euro beträgt;
- c. Rentenversicherungsverträge, sofern diese weder eine Rückkaufklausel enthalten noch als Sicherheit für ein Darlehen dienen können.

Durch die LV-SoV soll die Möglichkeit, vereinfachte Sorgfaltspflichten anzuwenden auch auf Versicherungsverträge im Rahmen der betrieblichen Altersvorsorge in all ihren Durchführungswegen (Betriebliche Kollektivversicherung gemäß § 93 VAG 2016, Zukunftssicherung gemäß § 3 Abs. 1 Z 15 lit. a Einkommensteuergesetz 1988, Pensionsrückdeckungsversicherung, Abfertigungsrückdeckungsversicherung, Abfertigungs- und Jubiläumsgeldauslagerungsversicherung), auf Verträge im Rahmen der prämienbegünstigten Zukunftsvorsorge gemäß §§ 108g ff EStG 1988 und auf Verträge im Rahmen der Pensionszusatzversicherung gemäß § 108b EStG 1988 ausgedehnt werden.<sup>25</sup>

##### 4.1.3.2.2 Anlage II Z 2 lit. d

72 Generell bedeutet „financial inclusion“ das Anbieten von Bank- und Finanzdienstleistungen an benachteiligte und ungeschützte Gruppen, wie z.B. Personen mit niedrigem Einkommen, Personen, die von der behördlichen Registrierung nicht erfasst sind sowie Personen, die vom formalen Finanzsektor nur sehr wenig bedient oder gar ganz ausgeschlossen werden. Da ein Leben ohne Girokonto in der Europäischen Union faktisch nicht mehr möglich ist, wurden mittels

<sup>24</sup> Begründung zu BGBl. II Nr. 1/2017, 2.

<sup>25</sup> Ebd.

der Richtlinie (EU) 2014/92/EU über die Vergleichbarkeit von Zahlungskontoentgelten, den Wechsel von Zahlungskonten und den Zugang zu Zahlungskonten mit grundlegenden Funktionen Bedingungen geschaffen, die allen Verbrauchern Zugang zu einem Zahlungskonto geben. Die unionsrechtlichen Vorgaben wurden in Österreich mit Inkrafttreten des Verbraucherzahlungskontogesetzes (VZKG<sup>26</sup>) umgesetzt.

**73** Steht einem Verbraucher bei Abschluss eines Rahmenvertrags über ein Zahlungskonto mit grundlegenden Funktionen kein amtlicher Lichtbildausweis iSd FM-GwG zur Verfügung und wird dieser daher durch einen Verpflichteten anhand von Dokumenten gemäß § 23 Abs. 6 VZKG identifiziert, so ist dies als zusätzlicher Risikofaktor zu berücksichtigen. Weitere Informationen zu Identitätsdokumenten von Asylwerbern, Asylberechtigten und Fremden ohne Aufenthaltsrecht siehe das **FMA-Rundschreiben zu den Sorgfaltspflichten zur Prävention von Geldwäscherei und Terrorismusfinanzierung, Stand: (Datum), Rz 64ff.**

#### 4.1.3.2.3 Anlage II Z 2 lit. e

**74** Im Rahmen der Umsetzung der Richtlinie (EU) 2018/843 („5. Geldwäsche-RL“) durch BGBl I Nr. 62/2019 wurde der bis dahin geltende § 46 FM-GwG aufgehoben und sind seit 01.01.2020 die Sorgfaltspflichten des FM-GwG auf alle E-Geldprodukte vollumfänglich anzuwenden.

#### 4.1.3.3 Risikofaktoren in geographischer Hinsicht

##### 4.1.3.3.1 Anlage II Z 3 lit. a

**75** Mitgliedstaaten und Staaten des EWR sind ein mögliches Anzeichen für ein potentiell geringes Risiko. Dies ergibt sich aufgrund der Verpflichtung zur Umsetzung der 4. Geldwäsche-RL. Dennoch sind bei diesen Ländern potentiell risikoe erhöhende Faktoren zu berücksichtigen, vgl. Rz 93ff.

##### 4.1.3.3.2 Anlage II Z 3 lit. b - d

**76** Zur Beurteilung des Risikos, das ein Drittland im Hinblick auf Geldwäscherei und Terrorismusfinanzierung darstellt, kann man z.B. auf folgende Dokumente oder Informationen als Hilfestellung zurückgreifen:

- a. Das Land ist Mitglied der FATF oder einer mit der FATF verbundenen regionalen Institution (sog. FSRB) wie z.B. MONEYVAL, Asia/Pacific Group on money laundering (APG), Grupo de Acción Financiera de Latinoamérica (GAFILAT), o.ä.
- b. Es sind Informationen von glaubwürdigen und vertrauenswürdigen Quellen über die Qualität der AML/CFT-Kontrollen der Jurisdiktion verfügbar, welche weiters Information über die Qualität der Effektivität der behördlichen Aufsicht und Vollstreckung beinhalten. Mögliche Quellen sind vor allem Mutual Evaluations der FATF oder FSRBs. Weiters können Länderprüfungen durch den Internationalen Währungsfond, Reports des Financial Sector Assessment Programme (FSAP) sowie Reports der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) herangezogen werden.
- c. Es liegen Informationen von glaubwürdigen und vertrauenswürdigen Quellen über den Umfang von Vortaten zur Geldwäscherei, wie z.B. Korruption, organisiertes Verbrechen oder Betrug vor. Dies sind z.B. der Transparency International's Corruption Perceptions Index (CPI);

<sup>26</sup> Verbraucherzahlungskontogesetz (VZKG), BGBl. II Nr. 255/2016, in der geltenden Fassung.

- die Länderreports der OECD betreffend Korruptionsbekämpfung: “Country reports on the implementation of the OECD Anti-Bribery Convention on the implementation of the OECD Anti-Bribery Convention“; UNODC World Drug Report.
- d. Es liegen Informationen von glaubwürdigen und vertrauenswürdigen Quellen im Hinblick auf die Kompetenz und Effektivität der Ermittlungsarbeit und des Justizwesens einer Jurisdiktion vor, Vorfälle entsprechend zu untersuchen und strafrechtlich zu verfolgen.
  - e. Die politische Lage des Landes ist stabil.
  - f. Es liegen Informationen von glaubwürdigen und vertrauenswürdigen Quellen im Hinblick auf die internationale Kooperation sowie den Informationsaustausch der Jurisdiktion mit ausländischen Behörden vor. Glaubhafte Quellen diesbezüglich sind z.B. Mutual Evaluations der FATF oder FSRBs sowie Reports des Forums on Transparency and Exchange of Information for Tax Purposes.

#### 4.1.4 Anlage III

77 Über die Anwendung der in Anlage I genannten Risikovariablen hinaus ist jedenfalls die Berücksichtigung der Risikovariablen der Anlage III bei jeder Risikoklassifizierung von Geschäftsbeziehungen erforderlich, da andernfalls durch den Verpflichteten nicht sichergestellt werden kann, dass allfällige Hochrisikokunden als solche erkannt und entsprechend einer verstärkten Überwachung unterzogen werden.

##### 4.1.4.1 Risikofaktoren bezüglich Kunden

###### 4.1.4.1.1 Anlage III Z 1 lit. a

78 Ob außergewöhnliche Umstände der Geschäftsbeziehung vorliegen, kann anhand u.a. folgender Faktoren bzw. Informationen beurteilt werden:

- a. Es liegen Hinweise vor, dass der Kunde versucht, die Begründung einer Geschäftsbeziehung zu umgehen.
- b. Erscheint die Eigentums- und Kontrollstruktur des Kunden transparent und sinnvoll? Für den Fall, dass die Eigentumsverhältnisse und Kontrollstruktur komplex und undurchsichtig sind, ist zu bewerten, ob hierfür eine klar erkennbare wirtschaftliche und/oder rechtliche Begründung vorliegt.
- c. Der Kunde verlangt die Durchführungen von komplexen, unüblich oder unerwartet hohen Transaktionen. Die durch den Kunden getätigten Transaktionen weisen ein unübliches oder unerwartetes Muster ohne offensichtlichen wirtschaftlichen oder rechtlichen Zweck oder eine fundierte kommerzielle Begründung auf. Es gibt Gründe, die vermuten lassen, dass der Kunde versucht, bestimmte Schwellenwerte zu umgehen.
- d. Der Kunde verlangt nicht erforderliche oder nicht angemessene Vertraulichkeitsstandards, KYC-Informationen werden nur zurückhaltend oder widerwillig zur Verfügung gestellt bzw. wird versucht, die Art des Geschäfts bzw. die Geschäftstätigkeit des Kunden zu verbergen.
- e. Unternehmensstrukturen mit Off-Shore-Beziehungen, Stiftungen, Treuhandschaften, Trusts oder andere Formen (z.B. nominee shareholder), die den wirtschaftlichen Eigentümer nicht klar erkennen lassen.
- f. Nicht auf Gewinn ausgerichtete Vereinigungen unter Berücksichtigung des Organisationszwecks, des Herkunftslandes bzw. Registrierungslandes und der Tätigkeit mit häufigen Zahlungen ins Ausland.
- g. Anträge auf Schließfachverträge von Personen, zu denen darüber hinaus keine Geschäftsbeziehung besteht.
- h. Transaktionen, die iZm Versicherungen getätigt werden, sollten den Ansprüchen der Unbedenklichkeit genügen. Sobald Elemente vorliegen, die eine Abweichung vom „vernünftigen Verhalten“ indizieren, sollten die Beweggründe dafür hinterfragt und glaubhaft gemacht werden. Dies betrifft insbesondere Bareinzahlungen und Rückkäufe, die zu unwirtschaftlichen Bedingungen erfolgen.

###### 4.1.4.1.2 Anlage III Z 1 lit. b

79 Zur Beurteilung von geografischen Gebieten mit hohem Risiko gemäß Z 3 der Anlage III siehe Ausführungen in den Rz 76 und Rz 93f.

## 4.1.4.1.3 Anlage III Z 1 lit. c

80 Obgleich vermögende Kunden nicht automatisch als verdächtig im Bereich der Geldwäscherei und Terrorismusfinanzierung angesehen werden sollen, besteht aufgrund der Größe der Vermögenswerte und der in manchen Fällen nur schwer nachvollziehbaren Mittelherkunft ein erhöhtes Risiko. Das besondere Vertrauensverhältnis, das zu vermögenden Privatkunden besteht, darf zu keiner Verringerung der Sorgfaltspflichten führen. Vielmehr sollte das objektive Risiko in die Kundenbewertung und das Kundenmonitoring einfließen.

Zum Risikofaktor juristische Personen oder Rechtsvereinbarungen, die als Instrumente für die private Vermögensverwaltung dienen, sind insbesondere folgende zu zählen: Stiftungen; Trusts bzw. trustähnliche Vereinbarungen und spezielle Investmentvehikel, insbesondere wenn der wirtschaftliche Eigentümer schwer festzustellen ist.

## 4.1.4.1.4 Anlage III Z 1 lit. d

81 Im Hinblick auf Unternehmen mit nominellen Anteilseignern oder als Inhaberpapieren emittierten Aktien ist speziell zu berücksichtigen, inwieweit die Feststellung und Überprüfung der wirtschaftlichen Eigentümer erschwert ist.

## 4.1.4.1.5 Anlage III Z 1 lit. e

82 Unternehmen, deren Geschäftstätigkeit verstärkt auf Bargeld ausgerichtet ist, können ein erhöhtes Risiko darstellen, da z.B. Bargeld, das durch kriminelle Handlungen erworben wurde, mit Erlösen einer legitimen Geschäftstätigkeit vermischt wird und auf diese Weise z.B. die Einzahlung der aus krimineller Tätigkeit stammenden Vermögenswerte auf ein Bankkonto ohne weitere Rückfragen durch die Bank möglich ist.

## 4.1.4.1.6 Anlage III Z 1 lit. f

83 Nähere Ausführungen zu dem Risikofaktor „angesichts der Art der Geschäftstätigkeit als ungewöhnlich oder übermäßig kompliziert erscheinende Eigentumsstruktur des Unternehmens“ siehe Rz 78b sowie Rz 78e.

## 4.1.4.1.7 Geschäftstätigkeit/Branche/Geschäftsmodell des Kunden

84 In den Anlagen nicht dezidiert angeführt ist der Risikofaktor „Geschäftstätigkeit/Branche/Geschäftsmodell des Kunden“. Es handelt sich bei den in den Anlagen I – III genannten Risikofaktoren jedoch nicht um eine erschöpfende Aufzählung und ist das Risikokriterium „Branche“ bzw. „Geschäftstätigkeit des Kunden“ bei der Risikoklassifizierung von Geschäftsbeziehungen jedenfalls miteinzubeziehen.

85 Zu berücksichtigten sind in diesem Zusammenhang u.a. folgende Informationen:

- a. Hat der Kunde oder der wirtschaftliche Eigentümer Verbindungen zu Sektoren, die gewöhnlich mit einem höheren Korruptionsrisiko assoziiert werden wie z.B. Baugewerbe, Pharmaindustrie und Gesundheitswesen, Waffenhandel und Verteidigung, Rohstoffabbau und -industrie oder öffentliche Auftragsvergabe?
- b. Hat der Kunde oder der wirtschaftliche Eigentümer Verbindungen zu Branchen, die mit einem höheren Risiko von Geldwäscherei und Terrorismusfinanzierung assoziiert werden, wie z.B. bestimmte „Money Service Businesses“, Casinos oder dem Handel von Edelmetallen?

- c. Hat der Kunde oder der wirtschaftliche Eigentümer Verbindungen zu einer besonders bargeldintensiven Branche?

4.1.4.1.8 Anlage III Z 1 lit. g

- 86 Risikofaktoren können auch Umstände wie folgt sein: der Kunde ist ein Drittstaatsangehöriger, der Aufenthaltsrechte oder die Staatsbürgerschaft eines Mitgliedstaats im Austausch gegen die Übertragung von Kapital, den Kauf von Immobilien oder Staatsanleihen oder Investitionen in Gesellschaften in diesem Mitgliedstaat beantragt;

4.1.4.2 Risikofaktoren bezüglich Produkten, Dienstleistungen, Transaktionen oder Vertriebskanälen

4.1.4.2.1 Anlage III Z 2 lit. a

- 87 Der in Z 2 lit. a der Anlage III genannte Risikofaktor „Banken mit Privatkundengeschäft“ umfasst die Betreuung vermögender Privatkunden, das sog. „Private Banking“. Ausführungen hierzu siehe Rz 80.

4.1.4.2.2 Anlage III Z 2 lit. b

- 88 Das Risiko von Transaktionen oder Produkten, die Anonymität begünstigen könnten, ist entsprechend zu berücksichtigen (z.B. E-Geldprodukte wie z.B. Prepaid-(Kredit)Karten).

4.1.4.2.3 Anlage III Z 2 lit. c

- 89 Anlage III Z 2 lit. c nennt Geschäftsbeziehungen oder Transaktionen ohne persönliche Kontakte und ohne bestimmte Sicherungsmaßnahmen als risikoe erhöhende Faktoren. Da § 6 Abs. 4 FM-GwG einen taxativen Katalog von Sicherungsmaßnahmen für das Ferngeschäft vorsieht, wird durch die Anwendung ebendieser Maßnahmen ein allfälliges erhöhtes Risiko ausgeglichen und ist die zusätzliche Berücksichtigung dieses Risikofaktors daher nicht erforderlich.

4.1.4.2.4 Anlage III Z 2 lit. d

- 90 Das Erkennen von Zahlungen von unbekanntem oder nicht verbundenen Dritten durch die Verpflichteten ist insbesondere bei Produkten bzw. Geschäftsbeziehungen mit vorhersehbarbarem Parteien- bzw. Personenkreis und daraus resultierendem vorhersehbarbarem Transaktionsverhalten von Relevanz. Dies ist insbesondere bei Produkten der Fall, im Rahmen derer schon aufgrund der Art und Beschaffenheit des Produktes regelmäßige Einzahlungen derselben Person(en) erfolgen: Versicherungsprämien, Ansparprodukte, wie z.B. Bausparen, Kreditrückzahlungen, Einzahlungen auf Konten von Miteigentumsgemeinschaften, etc.

4.1.4.2.5 Anlage III Z 2 lit. e

- 91 Zu den in Z 2 lit. e der Anlage III genannten Produkten und Geschäftsmodellen zählen insbesondere u.a. „mobile payments“, „peer-to-peer-Zahlungen“ sowie auf „Blockchaintechnologie“ basierende Produkte.

4.1.4.2.6 Anlage III Z 2 lit. f

- 92 Risikofaktoren können sich zudem auch wie folgt ergeben, z.B. Transaktionen in Bezug auf Öl, Waffen, Edelmetalle, Tabakerzeugnisse, Kulturgüter und andere Artikel von archäologischer, historischer, kultureller oder religiöser Bedeutung oder von außergewöhnlichem wissenschaftlichen Wert sowie Elfenbein und geschützte Arten;

#### 4.1.4.3 Risikofaktoren in geographischer Hinsicht

##### 4.1.4.3.1 Anlage III Z 3 lit. a - d

- 93 Welche glaubwürdigen und vertrauenswürdigen Quellen u.a. zur Bewertung von Länderrisiken im Hinblick auf Kriminalität, Korruption, Qualität der Strafverfolgung, etc. herangezogen werden können, siehe Ausführungen bei Rz 76 Punkte a - f.
- 94 Die Europäische Kommission legt mit delegierter Verordnung fest, zu welchen Ländern festgestellt wurde, dass nationale Systeme zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung strategische Mängel aufweisen<sup>27</sup>. Ist ein Kunde selbst oder ein wirtschaftlicher Eigentümer eines Kunden in einem solchen Land domiziliert, so sind durch die Verpflichteten jedenfalls verstärkte Sorgfaltspflichten anzuwenden. Des Weiteren sind ein- sowie ausgehende Transaktionen iZm diesen Ländern zu erkennen. Weitere Ausführungen diesbezüglich siehe **FMA-Rundschreiben zu den Sorgfaltspflichten zur Prävention von Geldwäscherei und Terrorismusfinanzierung, Stand: (DATUM), Rz 312ff.**

Darüber hinaus deuten folgende Umstände darauf hin, dass im Zusammenhang mit einem Land erhöhtes Risiko im Hinblick auf Geldwäscherei und Terrorismusfinanzierung vorliegt:

- a. politische Instabilität;
  - b. Länder, gegen die beispielsweise die Europäische Union oder die Vereinten Nationen Sanktionen, Embargos oder ähnliche Maßnahmen verhängt hat/haben;
  - c. es liegen Information von z.B. den Medien oder Strafverfolgungsbehörden darüber vor, dass Länder terroristische Aktivitäten finanziell oder anderweitig unterstützen oder in ihnen bekannte terroristische Organisationen aktiv sind;
  - d. bei dem Land handelt es sich um ein sog. „Steuerparadies“ („tax haven“); das Land verfügt über ein besonders strenges Bankgeheimnis („secrecy haven“) oder es handelt sich um eine Offshore-Destination, vgl. Rz 95f.
- 95 Ob es sich bei einer bestimmten Jurisdiktion um einen „tax haven“, einen „secrecy haven“ oder eine „Offshore-Destination“ handelt, ist immer Gegenstand einer Einzelfallprüfung.

Stark vereinfacht ist Offshore-Finanz die Bereitstellung von finanziellen Dienstleistungen durch Banken oder ähnliche Finanzdienstleister an Devisenausländer. Liegen die folgenden Merkmale vor, ist grundsätzlich von einem „tax haven“, einem „secrecy haven“ oder einer „Offshore-Destination“ auszugehen:

- a. in der betreffenden Jurisdiktion wird der Großteil der Aktivität des Finanzsektors auf beiden Seiten der Bilanz „offshore“ bereitgestellt (d.h., es handelt sich bei der Mehrzahl der beteiligten Banken bzw. Finanzdienstleister um Devisenausländer);
- b. Transaktionen werden andernorts initiiert und
- c. die Mehrheit der involvierten Institutionen werden von nicht-ansässigen Personen kontrolliert.

---

<sup>27</sup> Delegierte Verordnung (EU) 2016/1675 der Kommission vom 14. Juli 2016 zur Ergänzung der Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates durch Ermittlung von Drittländern mit hohem Risiko, die strategische Mängel aufweisen i.d.g.F.

- 96 Folgende weitere Merkmale sind Hinweise für einen „tax haven“, einen „secrecy haven“ oder eine „Offshore-Destination“:
- a. Es handelt sich um Jurisdiktionen, welche eine relativ große Anzahl an Banken bzw. Finanzinstituten aufweisen, welche hauptsächlich mit Devisenausländern Geschäftsbeziehungen unterhalten.
  - b. Das Finanzsystem inkl. externer Aktiva und Passiva steht außer Proportion zu den innerstaatlichen Bedürfnissen der Jurisdiktion und ist im Hinblick auf die Finanzierung deren Volkswirtschaft ausgelegt.
  - c. Wenn darüber hinaus eine oder alle der folgenden Voraussetzungen vorliegen:
    - niedrige oder keine Steuern;
    - hohe Standards betreffend das Bankgeheimnis und die Anonymitätswahrung;
    - moderate oder geringe Regulierungsstandards.

#### 4.1.5 Unternehmensspezifische Risikofaktoren

- 97 Die Aufzählung der Risikovariablen in den Anlagen I, II und III des FM-GwG ist nicht abschließend. Darüber hinaus ist es je nach Geschäftsmodell/Geschäftsumfeld, Größe und Komplexität der Geschäftstätigkeit eines Verpflichteten erforderlich, weitere unternehmensspezifische Risikofaktoren zu berücksichtigen. Insbesondere ist dies relevant, wenn z.B. Geschäftsbeziehungen begründet oder Produkte angeboten werden, die aus Sicht der Prävention von Geldwäscherei und Terrorismusfinanzierung ein erhöhtes Risiko darstellen, aber im Hinblick auf den Verpflichteten als spezifisch zu erachten sind und daher in den Anlagen I-III keine Berücksichtigung finden.

##### 4.1.5.1 Exkurs: Risikofaktoren im Bereich virtueller Währungen

- 98 Zur Ermittlung und Analyse der potentiellen Risiken der Geldwäscherei und Terrorismusfinanzierung im Bereich der virtuellen Währungen sind die Risikofaktoren in Verbindung mit der Produktart (Art der virtuellen Währung; anonyme virtuelle Währungen etc.), dem Geschäftsmodell (Art der Dienstleistung inkl. Vertriebswege) sowie den Transaktionen (inkl. technischer Möglichkeiten zur Verschleierung, z.B. „Mixing“ etc.) zu berücksichtigen (vgl. „FATF-Report Virtual Assets, Red Flag Indicators of Money Laundering and Terrorist Financing“, Stand 14.09.2020).
- 99 Zur Ermittlung und Analyse der potentiellen Risiken der Geldwäscherei und Terrorismusfinanzierung im Bereich der Dienstleister in Bezug auf virtuelle Währungen sind zumindest die nachfolgenden Punkte zu berücksichtigen:
- Internationale Standards und Dokumente zu virtuellen Währungen und Dienstleistungen bzw. Geschäftstätigkeiten im Bereich virtueller Währungen (bspw. von der FATF);
  - die immanenten Risiken von virtuellen Währungen, wie z.B. Dezentralität, Globalität und Marktunübersichtlichkeit, Anonymität, etc.;
  - das allgemeine Geschäftsumfeld des Unternehmens;

- die technischen Entwicklungen im Bereich virtueller Währungen, sowie Kursentwicklungen virtueller Währungen;
- die wesentlichen Risiken in diesem Zusammenhang bzw. das erhöhte Missbrauchspotential in Bezug auf virtuelle Währungen;
- das besondere Missbrauchspotential in Bezug auf Terrorismusfinanzierung.

#### 4.1.6 Gewichtung von Risikofaktoren

100 Für den Fall, dass der Verpflichtete bei der Risikoklassifizierung von Kunden Risikofaktoren gewichtet, sollte eine fundierte Beurteilung der Relevanz der unterschiedlichen Risikofaktoren im Kontext der Geschäftsbeziehung oder der Transaktion erfolgen. In der Praxis kann dies z.B. erfolgen, indem Risikovariablen „Scorepunkte“ zugeordnet werden; so könnte ein Verpflichteter z.B. die Entscheidung treffen, dass, unter Berücksichtigung der Eigenschaften eines durch den Kunden gewünschten Produktes, ein anderer Risikofaktor von geringerer Bedeutung ist.

101 Die Risikogewichtung wird daher je nach Produkt, Kunde oder Kundenkategorie sowie je nach Verpflichtetem variieren. Bei der Gewichtung von Risikofaktoren sollte Folgendes sichergestellt sein:

- a. die Gewichtung wird nicht übermäßig durch einen Risikofaktor beeinflusst;
- b. wirtschaftliche Überlegungen sowie Erwägungen betreffend Profit des Verpflichteten (nicht des Kunden) beeinflussen das Risikoring nicht;
- c. die Gewichtung führt nicht zu einer Situation, in der die Risikoklassifizierung einer Geschäftsbeziehung/Transaktion als „hohes Risiko“ nicht möglich ist;
- d. gesetzlich vorgegebene Anwendungsfälle erhöhten/hohen Risikos können durch unternehmenseigene Gewichtung nicht aufgehoben werden;
- e. es ist möglich, im Anlassfall automatisch generierte Risikoklassifizierungen zu überschreiben. Die Begründung für das Übersteuern einer Risikoklassifizierung sollte geeignet dokumentiert werden.

#### 4.1.7 Risikoklassifizierung mittels automationsunterstützter Systeme

102 Die Aufsichtspraxis der FMA hat gezeigt, dass es auf dem österreichischen Finanzmarkt üblich ist, dass Verpflichtete der Risikoklassifizierung von Geschäftsbeziehungen/gelegentlichen Transaktionen dienliche automationsunterstützte IT-Systeme nicht selbst entwickeln, sondern von externen Anbietern zukaufen. In diesem Fall ist es erforderlich, dass die Verpflichteten über ausreichend Kenntnis verfügen, wie das System funktioniert und auf welche Art und Weise die unterschiedlichen Risikofaktoren kombiniert bzw. zur gesamthaften Risikoklassifizierung zusammengeführt werden.<sup>28</sup>

103 Darüber hinaus ist es erforderlich, dass für jeden Verpflichteten die Möglichkeit besteht, bei den IT-Systemen zur Risikoklassifizierung und Überwachung institutsspezifische Gegebenheiten zu berücksichtigen. Bei Anwendung von z.B. in der Unternehmensgruppe vorgegebenen Systemen

---

<sup>28</sup> The Risk Factors Guidelines, Rz 38.

ist daher zumindest eine Evaluierung der Kalibrierung der Systeme im Hinblick auf die Institutsspezifika erforderlich.

## 5 ANHANG

### 5.1 Materialien<sup>29</sup>

- Richtlinie (EU) 2015/849 vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission („4. Geldwäsche-RL“).
- Richtlinie (EU) 2018/843 vom 30. Mai 2018 zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinien 2009/138/EG und 2013/36/EU („5. Geldwäsche-RL“).
- Leitlinien nach Artikel 17 und Artikel 18 Absatz 4 der Richtlinie (EU) 2015/849 über Sorgfaltspflichten und die Faktoren, die Kredit- und Finanzinstitute bei der Bewertung des mit einzelnen Geschäftsbeziehungen und gelegentlichen Transaktionen verknüpften Risikos für Geldwäsche und Terrorismusfinanzierung berücksichtigen sollten („Die Leitlinien zu den Risikofaktoren für Geldwäsche und Terrorismusfinanzierung“), zur Aufhebung und Ersetzung der Leitlinien JC/2017/37, März 2021 (EBA/GL/2021/02).
- Financial Action Task Force, Guidance for a risk-based approach – The banking sector, October 2014.
- Financial Action Task Force, International standards on combating money laundering and the financing of terrorism & proliferation – The FATF Recommendations, June 2021.
- Internationaler Währungsfonds (IWF), Enhancing Surveillance – Interconnectedness and Clusters, März 2012.
- FATF-Report Virtual Assets, Red Flag Indicators of Money Laundering and Terrorist Financing, September 2020.

*Anmerkung: Soweit Internetlinks in diesem Rundschreiben angegeben werden, ist dies ausschließlich zur Information. Die Richtigkeit der Links besteht zum Zeitpunkt der Beschlussfassung des Rundschreibens.*

---

<sup>29</sup> Dokumente der Financial Action Task Force (FATF) können von deren Homepage unter Publications abgerufen werden: <https://www.fatf-gafi.org/>.