

Geldwäscheprävention durch VT-Dienstleister

NICOLAS RASCHAUER/THOMAS STERN*

Abstract

Im Rahmen einer mehrteiligen Artikelserie werden zunächst wesentliche öffentlich-rechtliche Eckpunkte, daran anknüpfend einzelne zivilrechtliche Details des Regimes des TVTG, das seit 1. Jänner 2020 die Erbringung von VT-Dienstleistungen in Liechtenstein reglementiert, beleuchtet. Im vierten Teil der Artikelserie werden wesentliche Verhaltenspflichten der VT-Dienstleister nach SPG analysiert.

Schlagworte

Sorgfaltspflichtige, Sorgfaltspflichten, VT-Dienstleister, Token-Emittenten, Handelsplattformen, Geldwäscheprävention, Geldwäschebeauftragter, verstärkte Sorgfaltspflichten, vereinfachte Sorgfaltspflichten, Organisationspflichten, Sorgfaltspflichtkonzept, Geschäftsprofil, Identifikation, wirtschaftlich Berechtigter

Rechtsquellen

TVTG, SPG

Inhaltsübersicht

I.	Vorbemerkung	273
II.	Historische Entwicklung	273
III.	EWR-rechtlicher Hintergrund	273
IV.	Sorgfaltspflichtige	274
V.	Meldepflicht – Beginn der Sorgfaltspflichten	275
VI.	Sorgfaltspflichten-Allgemeines	275
VII.	Zu einzelnen Sorgfaltspflichten	277
	A. Feststellung und Überprüfung der Identität des Vertragspartners (Art 6 SPG; Art 6 ff SPV)	277
	B. Feststellung und Überprüfung der Identität der wirtschaftlich berechtigten Person und der Ausschüttungsempfänger (Art 7 ff SPG; Art 11 ff SPV)	278
	C. Geschäftsprofil (Art 8 SPG; Art 20 SPV)	279
	D. Risikoadequate Überwachung von Geschäftsbeziehungen (Art 9–9b SPG; Art 22 SPV)	281
	E. Abgleich hinsichtlich politisch exponierter Personen (PEP) (Art 11 Abs 4 SPG)	282
	F. Zeitpunkt der Wahrnehmung der Sorgfaltspflichten	283
	G. Mitteilungspflicht an die SFIU	283
	H. Dokumentation (Art 20 SPG; Art 27 ff SPV)	283
	I. Interne Organisation (Art 21 SPG; Art 31 ff SPV)	284
	1. Interne Weisungen (Art 21 Abs 1 SPG; Art 31 SPV)	285
	2. Aus- und Weiterbildung (Art 21 Abs 1 SPG; Art 32 SPV)	285
	3. Interne Funktionen (Art 22 SPG; Art 33 ff SPV)	285
	J. Sorgfaltspflichtkontrollen	286
VIII.	Risikomatrix nach SPG	287
	A. Risikobewertung (Art 9a SPG)	287

* Die in diesem Beitrag enthaltenen Meinungen repräsentieren ausschliesslich die privaten Auffassungen der Autoren, nicht aber jene ihrer Arbeitgeber.

B.	Risikoanalyse	288
C.	Zuordnung der Geschäftsbeziehungen und Transaktionen zu den Risikokategorien	289
D.	Festlegung wirksamer interner Kontroll- und Überwachungsmaßnahmen zur Minderung der Risiken	290
E.	Dokumentation und Aktualität der Risikobewertung	290
F.	Auswirkungen auf Sorgfaltspflichten des VT-Dienstleisters (Art 5 ff SPG)	290
IX.	Sanktionen	291
X.	Literatur	291

I. Vorbemerkung

Der gegenständliche Beitrag dient der Analyse der wesentlichen Sorgfaltspflichten von VT-Dienstleistern nach SPG. Dadurch soll, im Anschluss an die bisherigen Ausführungen zum TVTG, das Verständnis für die Stellung der VT-Dienstleister nach liechtensteinischem Recht erhöht werden.

II. Historische Entwicklung

Pkt 6.2. des VNB LNR 2018-879 für ein VTG sah vor, dass durch eine Novelle zu Art 3 SPG¹ der **Kreis der Sorgfaltspflichtigen um bestimmte VT-Dienstleister erweitert** werden sollte (Art 3 Bst r–w SPG idF des VNB. Erfasst werden sollten ua Token-Emittenten oder VT-Protektoren²).

Diese Entwurfsfassung wurde in der Vernehmlassung grds begrüsst (vgl zB BuA 2019/54, 302). Im Rahmen des BuA 2019/54 wurde zwecks Präzisierung des Anwendungsbereichs der Sorgfaltspflichten von VT-Dienstleistern mehrere **Begriffsdefinitionen** eingefügt (zB virtuelle Währung, VT-Wechseldienstleister; vgl ua Art 2 Abs 1 Bst l^{bis} und z^{bis} SPG idF BuA 2019/54).

Zudem präzisierten und modifizierten die Verfasser des BuA den **persönlichen Anwendungsbereich des Art 3 Abs 1 SPG**: Erfasst werden sollten nunmehr alle (registrierungspflichtigen) VT-Dienstleister und fachverwandte Tätigkeiten wie etwa Token-Emittenten, die keiner Registrierungspflicht gem TVTG unterliegen, sowie Betreiber von Handelsplattformen für virtuelle Währungen. Ergänzend wurde der **Umfang** der von VT-Dienstleistern zu prästierenden **Sorgfaltspflichten** (etwa durch Einfügung eines neuen Art 9b Abs 2a SPG) betreffend Transaktionsüberwachung klargestellt.

Im Rahmen der finalen Stellungnahme der Regierung an den Landtag zu den anlässlich der ersten Lesung betreffend das TVTG aufgeworfenen Fragen (BuA 2019/93), dh vor der 2. Lesung des TVTG im Landtag, nutzte die Regierung die Gelegenheit, die **Begriffsbestimmungen** des Art 2 SPG zu präzisieren bzw zu **beraignen** (etwa Streichung des Begriffes »Anbieter von elektronischen Geldbörsen«, da nunmehr die Tätigkeit des »VT-Schlüsselverwahrers« sorgfaltspflichtig sei und die Tätigkeit des Anbietens von elektronischen Geldbörsen unter den »VT-Schlüsselverwahrer« falle³).

Auch die Entwürfe zu Art 3 SPG idF BuA 2019/54 wurden präzisiert und erweitert. So wurde der Begriff

»Zahlungstoken« flächendeckend durch den neutraleren Begriff »Token« ersetzt. Für Betreiber von Handelsplattformen für virtuelle Währungen wurde eine **Meldepflicht** an die FMA **eingefügt** (Art 3 Abs 3 Bst i SPG neu⁴).

Zu den Art 5 Abs 2, 9b Abs 3 und Art 31 Abs 1 SPG bzw den korrespondierenden Erläuterungen fügte die Regierung im BuA Klarstellungen ein und korrigierte im Entwurfstext zur SPG-Novelle (bzw den Erläuterungen) verschiedene Verweisfehler.

III. EWR-rechtlicher Hintergrund

Im EWR definiert die **4. Anti-GW-RL (EU) 2015/849**,⁵ mittlerweile ins EWRA übernommen,⁶ die von den **Sorgfaltspflichtigen** zu prästierenden **Sorgfaltspflichten** zur Verhinderung von Geldwäsche und Terrorismusfinanzierung; darunter fallen auch VT-Dienstleister nach TVTG. Die entsprechenden Umsetzungsbestimmungen zu dieser RL finden sich insbesondere im SPG und in der Sorgfaltspflichtverordnung (SPV⁷). Dadurch werden die auch für Liechtenstein verbindlichen 40+9 FATF-Empfehlungen, auf denen die EU-RL 2015/849 und 2018/843 in weiten Teilen basieren, in nationales Recht übernommen.

Liechtenstein ist seit vielen Jahren aktives Mitglied von MONEYVAL. Dabei handelt es sich um den 1997 gegründeten Expertenausschuss des Europarats zur Bewertung nationaler Massnahmen gegen Geldwäscherei und Terrorismusfinanzierung. Dieses Regionalgremium nach Vorbild der FATF hat den Auftrag, durch wechselseitige Evaluierungen der einzelnen Mitgliedsstaaten sicherzustellen, dass deren Massnahmen gegen Geldwäscherei und Terrorismusfinanzierung den FATF-Standards entsprechen. MONEYVAL ist assoziiertes Mitglied der FATF und erstattet der FATF regelmässig Bericht.

Die konsolidierte 4. GW-RL stellt eine RL mit **Mindestharmonisierungscharakter** dar (vgl Art 5 der RL). Die RL lässt daher strengere nationale Ausführungsvorschriften (etwa hins der Ausweitung des Kreises der Sorgfaltspflichten) zu. Dies ist insb für den Umstand, dass Liechtenstein **VT-Dienstleister**, die für sich (noch) nicht EWR-rechtlich reguliert wurden, den **SPG-Standards**

4 Vgl BuA 2019/93, 66.

5 Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates 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, ABl (EU) 2015 L 141, 73, idF der RL (EU) 2018/843 [ABl [EU] 2018 L 156, 43].

6 Vgl EWR-Register Anh IX-23b.01 und 02.

7 LGBL 2009.98.

1 Gesetz vom 11. Dezember 2008 über berufliche Sorgfaltspflichten zur Bekämpfung von Geldwäscherei, organisierter Kriminalität und Terrorismusfinanzierung (Sorgfaltspflichtgesetz; SPG), LGBL 2009.47.

2 Vgl dazu auch die Erläut zu Art 3 SPG idF VNB, 131.

3 BuA 2019/93, 66.

unterwarf, von Bedeutung. Aus EWR-rechtlicher Sicht wäre die Einbeziehung der VT-Dienstleister, abgesehen von »Anbietern virtueller Geldbörsen« (Art 3 Nr 19 der 4. GW-RL), (noch) nicht erforderlich gewesen. Besonders bedeutend idZ erscheinen die eigens für VT-Dienstleister bzw VT-Systeme verankerten »Anhaltspunkte für Geldwäscherei« in Anhang 3 Kapitel E SPV.

IV. Sorgfaltspflichtige

Art 3 Abs 1 r–t SPG unterwirft folgende Personen/Unternehmen, die im Inland VT-Dienstleistungen erbringen und hier über einen Sitz oder Wohnsitz verfügen (vgl Art 12 TVTG), dem Anwendungsbereich des SPG:

i) **Art 3 Abs 1 Bst r SPG:** Die Mehrzahl der gem Art 12 Abs 1 TVTG registrierungspflichtigen VT-Dienstleister, wenn sie ihre Tätigkeit berufsmässig erbringen, konkret jene nach Art 2 Abs 1 Bst k und m–q bzw Bst u TVTG: Erfasst werden:

- Token-Emittenten, die ihre Tätigkeit berufsmässig erbringen (daher, wenn sie aufgrund der Erreichung der Schwellenwertgrenze gem Art 12 Abs 2 TVTG registrierungspflichtig sind);
- VT-Schlüssel-Verwahrer;
- VT-Token-Verwahrer;
- VT-Protektoren;
- physische Validatoren;
- VT-Wechseldienstleister;
- VT-Agenten.

Token-Erzeuger, VT-Prüfstellen, VT-Preisdienstleister und VT-Identitätsdienstleister werden den Bestimmungen des SPG nicht unterworfen. Dies ist darauf zurückzuführen, dass diese Dienstleistungen nicht auf Transaktionstätigkeiten, sondern einem unterstützenden Service (der Programmierung, nicht der Emission von Token; Prüfung, nicht Verfügung eines Tokens, usw) basieren, und diese im Rahmen ihrer üblichen Geschäftstätigkeit nicht mit Zahlungsmitteln oder ähnlichen Werten in Berührung kommen (siehe idZ zB Art 4 Abs 1 Ziff 18 ZDG⁸ [»Geld«] bzw Art 2 Abs 1 Bst z^{bis} SPG [»virtuelle Währung«]).

ii) **Art 3 Abs 1 Bst s SPG:** Nicht gem Art 12 Abs 2 TVTG registrierungspflichtige Token-Emittenten, wenn sie den Schwellenwert von CHF 1.000 (egal ob eine oder mehrere kumulative Emissionen) oder mehr erreichen. Token-Emittenten sind Personen, die Token (Art 2 Abs 1 Bst c TVTG) im eigenen Namen oder im Namen eines

Auftraggebers öffentlich anbieten (Art 2 Abs 1 Bst k TVTG). Eine Begründung für die Schwellenwerthöhe von CHF 1.000 liefern die Erläuterungen nur in Bezug auf den allgemeinen FATF-Standard (zB Stellungnahme der Regierung 2019/93, 67f; BuA 2019/54, 307f). Für die Berechnung der möglichen Erreichung des Schwellenwertes erscheint die Höhe der konkreten Gegenleistung von Relevanz (»Kaufpreis« der Token), nicht der (zB im Rahmen einer Roadshow geschätzte) Wert der Token (s den Wortlaut »Verkaufspreis« in Art 31 Abs 1 Bst c TVTG). Bei schwankenden Wechselkursen (zB Token vs Fiat/Token) ist uE auf den Zeitpunkt der Emission abzustellen. Nachträgliche Wertveränderungen der Token haben keine Auswirkungen auf die Erreichung oder Nichterreichung des Schwellenwertes.

iii) **Art 3 Abs 1 Bst t SPG: Betreiber von Handelsplattformen für virtuelle Währungen** (Art 2 Abs 1 Bst z^{bis} SPG) bzw Token. Erfasst werden grds jene Personen, die Handelsplattformen betreiben, über die ihre Kunden einen Wechsel von virtuellen Währungen bzw Token gegen gesetzliche Zahlungsmittel oder andere virtuelle Währungen bzw Token und umgekehrt abwickeln oder abwickeln lassen. Von der Definition werden die Betreiber umfasst, wenn ihre Tätigkeit über eine blosse Vermittlungstätigkeit ohne Einbezug in die Zahlungsflüsse der Plattformnutzer hinausgeht, die jedoch weder Token noch VT-Schlüssel für ihre Kunden verwahren (vgl Art 2 Abs 1 Bst z^{ter} SPG). Eine »blosse Vermittlungstätigkeit« führt damit nicht zur Erfüllung der SPG-Definition, und somit auch nicht zur Unterwerfung unter die Sorgfaltspflichten des SPG. Unter die blosse Vermittlungstätigkeit fällt die reine Namhaftmachung möglicher Käufer und Verkäufer, auch wenn diese granular nach selektiven Kriterien gefiltert werden. Dies gilt, solange kein »Einbezug in die Zahlungsflüsse der Plattformnutzer« stattfindet, dh der Betreiber Token oder Gelder zwischen den Nutzern umbucht (*»direkte Verfügungsmacht über fremde Vermögenswerte haben bzw. eingeräumt erhalten«*; BuA 2019/54, 304). Eine »Abschlussvermittlung« (Anschaffung oder Veräusserung von Token im fremden Namen für fremde Rechnung) durch den Betreiber dürfte die Ausnahme der »blossen Vermittlung« hingegen tendenziell ausreizen und den Betreiber zu einem Sorgfaltspflichtigen befördern. Bedeutend erscheint, dass der Gesetzgeber insb die »Betreiber von Schnittstellen (bspw Webseiten), welche lediglich eine vereinfachte Nutzung ermöglichen, insb durch graphische Aufbereitung der sogenannten decentralized exchanges (Dex), welche gerade keine Betreiber haben« (BuA 2019/54, 304f) von der Definition ausnehmen wollte. Die Definition ist gesetzlich aber deutlich enger gefasst, wodurch Handelsplattformen, die keinen Zugriff auf die »Wallets« bzw die Konten der Nutzer haben, nicht unter

8 Zahlungsdienstegesetz (ZDG) vom 6. Juni 2019, LGBI 2019.213.

die SPG-Definition eines »Betreibers von Handelsplattformen für virtuelle Währungen« fallen.

In keinem Fall handelt es sich bei den beschriebenen Aktivitäten (Handelsplattform für virtuelle Währungen/Token, ungeachtet ob blosser Vermittlung oder nicht) um einen VT-Dienstleister nach Art 2 Abs 1 Bst i TVTG.

iv) Davon getrennt zu sehen sind Personen, die mit **Gütern handeln**, soweit die Bezahlung in bar oder mittels einer virtuellen Währung bzw eines Token erfolgt und sich der Betrag auf zumindest CHF 10.000 beläuft (Art 3 Abs 1 Bst q SPG). Sie sind nicht als VT-Dienstleister klassifiziert und werden nachfolgend nicht näher behandelt.

v) **Sonstiges:** Ausländische Personen/Unternehmen, die VT-Dienstleistungen ohne Zweigniederlassung/Repräsentanz in Liechtenstein erbringen (zB Emissionsofferte eines Token-Anbieters aus dem EWR-Ausland oder Drittstaat über ein Onlineportal), unterliegen nicht dem TVTG (Art 12 Abs 1 TVTG) und damit auch nicht dem SPG. Anbieter mit Sitz in Liechtenstein haben im Vergleich zu ausländischen Anbietern aufgrund des zusätzlichen Aufsichtsregimes (TVTG, SPG, sofern der Anbieter nicht im Herkunftsstaat sorgfaltspflichtig ist) einen Wettbewerbsnachteil.

Zu beachten ist, dass VT-Dienstleister ab dem 1. Januar 2020 auch dann dem SPG unterstehen, wenn sie sich noch nicht bei der FMA registriert haben (beachte idZ Art 50 Abs 1 TVTG).

V. Meldepflicht – Beginn der Sorgfaltspflichten

Als Grundregel ergibt sich aus Art 19 Abs 5 TVTG, dass **VT-Dienstleister**, die nach TVTG registrierungspflichtig sind, **ihre Tätigkeit erst nach erfolgter Eintragung** in das VT-Dienstleisterregister der FMA **aufnehmen dürfen; spätestens⁹ ab diesem Zeitpunkt unterliegen die Dienstleister nach Art 3 Abs 1 Bst r SPG den Sorgfaltspflichten** des SPG (s auch unten VI.). Die FMA als zuständige Aufsichtsbehörde (Art 23 SPG iVm Art 39 TVTG), welche die relevanten Eintragungen in das Dienstleisterregister vorzunehmen hat (Art 19 Abs 3 TVTG), weiss daher exakt, wann die angesprochenen VT-Dienstleister ihre Tätigkeiten operativ aufnehmen. **Sorgfaltspflichten bei**

9 Art 3 Abs 1 Bst r SPG adressiert explizit »registrierungspflichtige«, nicht »registrierte« Anbieter. Die SPG-Bestimmungen gelten schon dann, wenn ein Anbieter seine Dienstleistungen ohne Eintragung in das Register durchführt, sofern er zur Eintragung verpflichtet war. Der Fall könnte dann beispielweise dann eintreten, wenn zwischen dem (schon tätigen) Anbieter und der FMA Meinungsverschiedenheiten zu den Inhalten der Tätigkeit oder zum »Sitz« des Unternehmens bestehen (vgl unten im Text).

registrierungspflichtigen VT-Dienstleistern (Art 3 Abs 1 Bst r SPG) **sind unabhängig von bestimmten Schwellenwertgrenzen bzw Transaktionszahlen/-volumina einzuhalten** (Art 5 Abs 2 Bst g SPG).

Anderes gilt für VT-Wechseldienstleister, die erst ab einem Transaktionsvolumen von CHF 1.000 sorgfaltspflichtig sind (Art 5 Abs 2 Bst h SPG).

Davon wiederum zu unterscheiden sind Personen gem Art 3 Abs 1 Bst s und t TVTG: In diesem Zusammenhang ordnet Art 3 Abs 3 Bst h und i SPG an, dass **nicht-registrierungspflichtige Token-Emittenten** (Art 3 Abs 1 Bst s SPG) und **Betreiber von Handelsplattformen** für virtuelle Währungen bzw Token (Art 3 Abs 1 Bst t SPG) die Aufnahme ihrer Tätigkeit der FMA schriftlich anzuzeigen haben. Dadurch wird gewährleistet, dass die FMA als zuständige Aufsichtsbehörde auch bei jenen Personen, die keiner Registrierungspflicht nach TVTG unterliegen, dennoch Kenntnis über den Beginn der operativen Tätigkeit erhält. Ohne entsprechende Meldepflicht würde die FMA nicht bzw nicht sofort Kenntnis von der Aufnahme der einschlägigen Geschäftstätigkeit erhalten, »*was der Erfüllung ihrer aufsichtsbezogenen Aufgaben abträglich wäre*«. ¹⁰

Die Anbieter gelten jedoch schon ab Erfüllung der jeweiligen »Definition« in Art 3 Abs 1 SPG als »Sorgfaltspflichtige«. Faktisch werden die Verpflichtungen regelmässig erst ab **vollständigem Einlangen der Anzeige bei der FMA relevant, da die Unternehmen erst ab diesem Zeitpunkt tätig werden dürfen**, insb bei der Aufnahme einer Geschäftsbeziehung oder bei der Abwicklung von gelegentlichen Transaktionen (Art 5 Abs 2 Bst a und b SPG). Abgrenzungsprobleme können zB entstehen, wenn der Eigentümer des Betreibers schon vor der Anzeige an die FMA wie ein »Kunde« agiert und Transaktionen am Markt, womöglich auch nur zu Testzwecken im Rahmen einer Roadshow, durchführen lässt. Mangels einschlägiger Ausnahme im SPG wären auch solche Vorgänge durch den Betreiber trotz ausstehender Anzeige im Lichte der Sorgfaltspflichten (»Aufnahme einer Geschäftsbeziehung«, hier konkret mit dem Eigentümer) zu prüfen (vgl Art 5 Abs 2 Bst a SPG).

VI. Sorgfaltspflichten-Allgemeines

Sorgfaltspflichtige **VT-Dienstleister** mit Sitz oder Wohnsitz in Liechtenstein, die einschlägige VT-Dienstleistungen in Liechtenstein erbringen, sowie Unternehmen nach Art 3 Abs 1 Bst s und t SPG unterliegen spätestens ab Registrierung bzw entsprechender Anzeige an die FMA (Art 3 Abs 3 SPG; Art 19 Abs 5 TVTG) dem Geldwäschepräventionsregime nach SPG bzw SPV (zur folgen-

10 BuA 2019/93, 67.

den Darstellung vgl ausserdem die einschlägigen FMA-Wegleitungen, Richtlinien und Mitteilungen zum SPG).

VT-Dienstleister haben grundsätzlich sämtliche **Sorgfaltspflichten eigenständig zu erfüllen**.

Davon ist die Auslagerung von Sorgfaltspflichten oder die vertragliche Beauftragung von Dritten im Sinn der Art 14 SPG; 24 ff SPV zu unterscheiden. Erbringen Dritte für VT-Dienstleister Sorgfaltspflichten (etwa ein beauftragter Rechtsanwalt), bleibt der VT-Dienstleister dennoch im Aussenverhältnis für die Einhaltung der Sorgfaltspflichtstandards nach SPG verantwortlich.¹¹ Zu betonen ist, dass auch registrierungspflichtige VT-Dienstleister als »Dritte« iSd Art 14 Abs 1 Bst a SPG gelten können.¹²

Gem Art 5 Abs 1 SPG haben VT-Dienstleister zu gewährleisten:

- ▶ die Feststellung und Überprüfung der **Identität des Vertragspartners** bzw VT-Nutzers (Art 6 SPG);
- ▶ die Feststellung und Überprüfung der **Identität der wirtschaftlich berechtigten Person** (Art 7 SPG);
- ▶ die Feststellung und Überprüfung der **Identität des Ausschüttungsempfängers** diskretionär ausgestalteter Rechtsträger und des Begünstigten von Lebensversicherungen und anderer Versicherungen mit Anlagezweck (Art 7a und 7b SPG);
- ▶ die **Erstellung eines Geschäftsprofils** des VT-Nutzers (Art 8 SPG); sowie
- ▶ die **risikoadäquate Überwachung der Geschäftsbeziehung** (Art 9 SPG).

Die Vorgaben des SPG erscheinen auf den ersten Blick technologieneutral, insb wenn Art 9b SPG die »Verwendung informatikgestützter Systeme« für alle Sorgfaltspflichtigen fordert. Im Lichte von Art 9b Abs 2a SPG wird jedoch deutlich, dass VT-Dienstleister einem strengeren Regime unterworfen werden, insb durch die ergänzende Verpflichtung zum Monitoring der Historie von Token (Art 9b Abs 2a SPG iVm Art 21 Abs 2 SPV). Zudem gilt für VT-Dienstleister der Schwellenwert in Art 21 Abs 1 SPG (*»Die Sorgfaltspflichtigen haben ab einer Gesamtzahl von 100 verwalteten Geschäftsbeziehungen ein informatikgestütztes System zur Ermittlung von Geschäftsbeziehungen und Transaktionen mit politisch exponierten Personen zu verwenden«*) nicht (Art 21 Abs 1 Satz 2 SPG). Das SPG ist in dieser Hinsicht somit **nicht völlig technologieneutral**, da sorgfaltspflichtige (registrierungspflichtige) VT-Dienstleister strengeren Anforderungen unterliegen als andere Sorgfaltspflichtige. Dies gilt sogar dann, wenn letztere ebenso auf VT-Systemen tätig sind, aber keine

Rolle nach Art 3 Abs 1 Bst r SPG iVm Art 2 Abs 1 TVTG erfüllen (zB Bank mit Sitz in Liechtenstein, die als Token-Erzeuger, Prüfstelle und/oder Identitätsdienstleister registriert ist).

In welchem **Umfang** VT-Dienstleister Sorgfaltspflichten erfüllen müssen, bestimmt sich nach dem mit einer einzelnen **Geschäftsbeziehung** oder gelegentlichen Transaktion **verknüpften Risiko**. Nach Art 10 SPG können in Fällen mit geringem Risiko auf Geldwäscherei, organisierte Kriminalität und Terrorismusfinanzierung »vereinfachte Sorgfaltspflichten« angewandt werden.

Im Fall von erhöhten oder hohen Risiken im Sinne von Art 11 SPG sind entsprechend verstärkte Sorgfaltspflichten anzuwenden. **Anhang 3 Kapitel E SPV** legt eigens für VT-Dienstleister eine demonstrative Liste an Sachverhalten offen, bei denen Anhaltspunkte für Geldwäscherei unterstellt werden, zB **VT-Systeme, die erhöhte Anonymität erlauben** (Anhang 3 Kapitel E Ziff 1, 21 und 22 SPV).

VT-Dienstleister haben daher pro Geschäftsfall einen »risikobasierten Ansatz« anzuwenden. (vgl dazu FMA-Richtlinie 2013/1). Einen selbstregulatorischen Mindeststandard kann das VT-System selbst schaffen, in dem dieses zB bestimmte Kundengruppen, Zielmärkte oder Produkte präventiv von der Integration im VT-System technisch ausschliesst. Dies kann es den VT-Dienstleistern erleichtern, innerhalb der Restmenge einen risikobasierten Ansatz stärker zu verfolgen (zB Durchführung der Risikobewertung nach Art 9a SPG, Identifikation verbotener Geschäftsbeziehungen oder Produkte nach Art 13 SPG) und/oder die Erfüllung bestimmter Aufgaben an zulässige Dritte (Art 14 SPG) zu delegieren.

VT-Dienstleister haben die **Einhaltung** der unternehmens- bzw gruppeninternen Implementierung der **Sorgfaltspflichten** umfassend zu **dokumentieren**, wobei gerade auf VT-Systemen die Dokumentation des VT-Dienstleisters mit den Transaktionsdaten des Systems (Token-Historie) übereinstimmen muss. Die Erarbeitung, Herausgabe und Nachvollziehbarkeit der Dokumentation muss auch »off-line« jederzeit effektiv möglich sein, ebenso wie die Korrektur fehlender oder falscher Angaben. Um die Einhaltung der SPG-Compliancevorgaben zu gewährleisten, müssen VT-Dienstleister somit eine adäquate interne Organisationsstruktur einrichten (Art 21 f SPG), die im Grundsatz auch ohne das VT-System funktionieren kann (zB im Fall des Systemausfalls oder bei Cyberangriffen). Bei Verdacht auf Geldwäsche sind VT-Dienstleister verpflichtet, eine Verdachtsmeldung bei der Stabstelle FIU zu erstatten (Art 17 SPG). Erforderlichenfalls sind weitere Transaktionen im Rahmen einer aufrechten Geschäftsbeziehung zu unterlassen zw die Fortführung der Geschäftsbeziehung zu sistieren, was ua die unverzügliche Sperrung

¹¹ Dazu weiterführend N. Raschauer/Stern, LJZ 2020, 156 ff.

¹² Zu den »Dritten« vgl Herzog in *Achtelik/Herzog*, GWG-Kommentar³ § 17 Rz 7.

von Bankkonten erforderlich machen kann (Art 18 SPG). VT-Dienstleister haben bei Teilnahme in einem VT-System vorab sicherzustellen, dass die Wahrnehmung ihrer rechtlichen Dokumentationsverpflichtungen jederzeit möglich ist und auch durch Änderungen des Programmcodes nicht behindert werden kann.

VII. Zu einzelnen Sorgfaltspflichten

A. Feststellung und Überprüfung der Identität des Vertragspartners (Art 6 SPG; Art 6 ff SPV)

VT-Dienstleister haben ihre **Vertragspartner** sowohl bei **Beginn einer Geschäftsbeziehung** (zB bei der Emission, Verwahrung oder treuhänderischen Verwaltens von Token) als auch bei einer gelegentlichen Transaktion (zB Wechsel von Token in gesetzliche Zahlungsmittel) **festzustellen** und zu **überprüfen**. Entstehen im Lauf der Geschäftsbeziehung Zweifel über die Identität des Vertragspartners, so müssen VT-Dienstleister die Feststellung und Überprüfung der Identität des Vertragspartners wiederholen. Die Identität ist anhand aktueller, beweiskräftiger Dokumente (zB Reisepass, Handelsregisterauszug) zu überprüfen. Die Feststellung der Identität kann durch das VT-System aktiv **unterstützt** werden, zB durch eine historische Datensammlung zum Nutzer (Überprüfung der Identität, wesentliche Änderungen in den Stammdaten, Transaktionsverhalten). Eine Substitution gesetzlicher Verpflichtungen mit Berufung auf ein VT-System findet jedoch nicht statt. Beispielsweise darf sich ein sorgfaltspflichtiger VT-Dienstleister in SPG-Belangen nicht ausschliesslich auf die Aussagen eines VT-Identitätsdienstleisters (»Person, die den Verfügungsberechtigten eines Token identifiziert«) verlassen. Da letztere Rolle selbst nicht dem SPG unterfällt (vgl Art 2 Abs 1 Bst t TVTG iVm Art 3 Abs 1 Bst r SPG) scheidet auch eine Delegation nach Art 14 Abs 1 SPG aus, wodurch die Rolle des VT-Identitätsdienstleisters auf VT-Systemen nicht nur normativ, sondern auch faktisch sehr stark eingeschränkt sein dürfte.¹³ Auch für die ausschliessliche Berufung zur Erfüllung der SPG-Pflichten durch die Existenz »dezentraler Buchführung« besteht keine Rechtsgrundlage.

Bei **natürlichen Personen** genügt die **einmalige Identifikation** des Kunden für alle nachfolgenden Geschäftsbeziehungen. Das jeweilige Identifikationsdokument, sprich das beweiskräftige Dokument, muss dabei

bei allen nachfolgend aufgenommenen Geschäftsbeziehungen gültig sein (Art 7 SPV). Auch auf VT-Systemen muss die Zuordnung zu natürlichen Personen jederzeit möglich sein. Pure Verweise auf IT-Adressen oder Wallets (zB anonyme Nutzer einer Bitcoin-Blockchain) reichen nicht aus.¹⁴

VT-Dienstleister haben in diesem Zusammenhang zu gewährleisten, dass die von ihnen erhobenen Dokumente in »Sorgfaltspflichtakten« erfasst werden (Art 20 SPG). Diese Akten müssen vollständig sein, sodass insbesondere auch Änderungen in der Geschäftsbeziehung bzw in der Dokumentation nachvollzogen werden können. Dabei ist es zulässig, dass für mehrere Sorgfaltspflichtakten relevante Dokumente, wie beispielsweise die Kopie des Originals oder der echtheitsbestätigen Kopie des beweiskräftigen Dokuments, an einem zentralen Ort aufbewahrt werden, sofern die zentrale Aufbewahrung aus dem jeweiligen Sorgfaltspflichtakt eindeutig ersichtlich ist. Auf VT-Systemen bestünde zudem die zusätzliche Möglichkeit der Abbildung der Kopien auf dezentralen Hauptbüchern, sofern die gesetzlichen Bestimmungen (neben SPG insbesondere bezogen auf Geheimnis- und Datenschutz) eingehalten werden können.

Handelt es sich beim Vertragspartner um einen **Rechtsträger (juristische Person)**, dürfen die Dokumente bei Aufnahme jeder neuen Geschäftsbeziehung **nicht älter als zwölf Monate** sein, um die Aktualität sicherzustellen (Art 10 Abs 3 SPV). Jedoch genügt auch hier das einmalige Einholen der Dokumentation für mehrere Geschäftsbeziehungen, sofern gewährleistet ist, dass die Dokumente nicht älter als zwölf Monate sind. Auch hier haben VT-Dienstleister Sorgfaltspflichtakten zu führen, die vollständig und aktuell sein müssen. VT-Systeme könnten hier derart ausgestaltet werden, dass diese die Nutzung des Systems verbieten oder Nutzer individuell ausschliessen, wenn die Aktualität der Dokumente (zB bei Monitoring über Smart Contracts) nicht gegeben ist.

Gemäss Art 6 Abs 1 Bst b SPV sind bei Rechtsträgern ua die Namen der für den Rechtsträger im Verhältnis zum Sorgfaltspflichtigen formell handelnden **Organe** oder Trustees zu erheben und zu dokumentieren. Festzustellen sind aber nur diejenigen Personen, die gegenüber

13 Dies insbesondere deswegen, da VT-Dienstleister die SPG-Bestimmungen entweder originär erfüllen oder sich, womöglich neben einem VT-Identitätsdienstleister, noch einen Sorgfaltspflichtigen zur Delegation suchen müssten. Die Problematik wird aufgelöst, wenn sich die Sorgfaltspflicht durch einen anderen SPG-Tatbestand ergibt, beispielsweise eine Bank als VT-Identitätsdienstleister registriert wurde.

14 Gerade bei solchen Systemen erscheint fraglich, ob diese seitens der FMA als »VT-System« (»vertrauenswürdige Technologien«) anerkannt werden dürfen. Diese erfüllen zwar womöglich die Begriffsdefinition nach Art 2 Abs 1 Bst b TVTG, erschweren oder verunmöglichen aber, je nach System, die effektive Sicherstellung der Einhaltung von SPG-Sorgfaltspflichten. Da das »System« selbst nicht Normadressat des TVTG ist (und auch keine Vorgabe besteht, wonach VT-Systeme »gesetzeskonform« sein müssten), könnte dies durch die FMA nur bei der Registrierung der Nutzer auf diesem System problematisiert werden (vgl Art 18 Abs 1 Bst c TVTG).

dem Sorgfaltspflichtigen im Rahmen der Aufnahme der Geschäftsbeziehung konkret auftreten und den Vertragspartner vertreten (zB die Organe, die für den Rechtsträger die schriftliche Erklärung nach Art 11 SPV abgeben), nicht zwingend aber die gesamte Geschäftsleitung.

VT-Dienstleister haben sicherzustellen, dass jede Person, die angibt, für den Vertragspartner zu handeln, hierzu ermächtigt ist. Dies kann beispielsweise durch Einsichtnahme in eine Vollmacht oder einen aktuellen Handelsregisterauszug erfolgen. VT-Dienstleister haben die Identität solcher Personen durch Dokumentation der Angaben nach Art 6 Abs 1 Bst a SPV festzustellen und diese Daten mittels Einsichtnahme in ein beweiskräftiges Dokument (Original oder echtheitsbestätigte Kopie) zu legitimieren (Art 9 SPV). Zu beachten ist, dass die Registrierung als VT-Dienstleister allein nicht zur Legitimierung nach Art 9 SPV (»Echtheitsbestätigung«) ermächtigt. Eine alleinige reine Berufung auf die Mechanismen des VT-Systems (zB mehrfache Identifizierung durch andere Nutzer bzw Identifizierungs- und Dokumentationskette) gilt nicht als Erfüllung der gesetzlichen Bestimmungen.

Von den beweiskräftigen Dokumenten sind jeweils **Kopien** des Originals oder der echtheitsbestätigten Kopie **anzufertigen** und nach Art 10 Abs 2 SPV mit einer Bestätigung, dass das Original oder die echtheitsbestätigte Kopie eingesehen wurde, zu versehen, zu unterzeichnen, zu datieren sowie zum jeweiligen Sorgfaltspflichtigen (vorbehaltlich einer zentralen Aufbewahrung oder Mehrfachkopierung im dezentralen System) zu nehmen.

VT-Dienstleister haben die Dokumentation zur Feststellung und Überprüfung des Vertragspartners zu unterzeichnen und zu datieren. Als Unterschrift gilt hierbei auch die Verwendung eines individualisierten Stempels, welcher beispielsweise das Kurzzeichen des entsprechenden Mitarbeiters samt dessen Visum enthält.

Die Unterschrift kann auch von einem Beschäftigten eines VT-Dienstleisters geleistet werden, sofern er nach der internen Organisation des Unternehmens hierzu ermächtigt ist (zB durch interne Weisung).

In der Regel sollte die Dokumentation von jenem Beschäftigten unterschrieben werden, der die Geschäftsbeziehung aufnimmt oder massgeblich in diesen Prozess involviert ist. Sollten anlässlich einer Kontrolle Fragen zu der Dokumentation entstehen, wird die FMA unter Umständen den Kontakt zu diesem Beschäftigten herstellen wollen. Es ist sohin zu gewährleisten, dass für einen externen Dritten der Zeichnende der Dokumentation erkennbar ist (zB durch Anführung des Namens in leserlicher Schrift bzw Maschinenschrift unterhalb der Unterschrift).

Als weitere Möglichkeit kommt eine elektronisch »unterschriebene« Dokumentation in Betracht. Bei dieser Möglichkeit muss die Authentizität der »Unterschrift« im Sorgfaltspflichtigen gewährleistet sein. Dies

bedeutet: Eine Unterschrift kann nicht von mehreren Personen gesetzt werden, sondern nur von dem unterschreibenden Beschäftigten bzw Sorgfaltspflichtigen selbst. Umgehungsmöglichkeiten müssen weitestgehend ausgeschlossen werden, zB mit mehrfach gesicherten Zugriffssperren (Passwort, TAN, usw). VT-Dienstleister haben daher durch systematische Vorkehrungen sicherzustellen, dass automatisiert und unveränderbar dokumentiert wird, wann welcher Mitarbeiter ein Dokument überprüft hat, wobei eine dezentrale Kontrolle über mehrere Hauptbücher dem grundsätzlich nicht entgegensteht.

In allen vorgenannten Fällen gilt, dass für einen externen Dritten (zB andere VT-Dienstleister am VT-System, Aufsichtsbehörde) der Zeichnende der Dokumentation erkennbar sein muss.

Echtheitsbestätigungen können gemäss Art 9 SPV von einer Zweigstelle oder Konzerngesellschaft der VT-Dienstleister oder von einem anderen Sorgfaltspflichtigen nach Art 3 Abs 1 Bst a-i SPG (zB einem Treuhänder) ausgestellt werden.

B. Feststellung und Überprüfung der Identität der wirtschaftlich berechtigten Person und der Ausschüttungsempfänger (Art 7 ff SPG; Art 11 ff SPV)

Die Feststellung und Überprüfung der Identität der wirtschaftlich berechtigten Personen hat in einem gestuften Prozess zu erfolgen.

1. Schritt: Feststellung und Überprüfung der Identität der wirtschaftlich berechtigten Person;
2. Schritt: Feststellung und Überprüfung der wirtschaftlichen Berechtigung.

Im **ersten Schritt** haben VT-Dienstleister die **Identität** der in einer Geschäftsbeziehung bzw der an einer Transaktion **wirtschaftlich berechtigten Person** festzustellen (Art 7 Abs 1 SPG). Die Identität der wirtschaftlich berechtigten Person ist sowohl bei Beginn einer Geschäftsbeziehung (zB Beginn des Protektorats über Token) als auch bei einer gelegentlichen Transaktion festzustellen und zu überprüfen. Die verpflichtende transparente Darstellung aller wirtschaftlichen Berechtigten sämtlicher Nutzer des VT-Systems (dh Kunden [Verfügungsberechtigte], andere VT-Dienstleister) dürfte regelmässig eine konkludente »Eintrittsvoraussetzung« für das Funktionieren eines VT-Systems generieren (dh nur vollständige transparente Nutzer erhalten Zugang zum System; Dokumente werden nach SPG-Vorgaben zentral/dezentral legitimiert, usw; vgl Anhang 3 Kapitel E Ziff 1 SPV).¹⁵

¹⁵ Andernfalls könnten die, durch fehlende Synergien verursachten Kosten (jeder sorgfaltspflichtige Nutzer beschafft Dokumente

Zur gesetzeskonformen Identifizierung hat der Sorgfaltspflichtige die **Angaben nach Art 6 Abs 1 Bst a SPV** zu erheben und zu dokumentieren. Die Angaben sind durch risikobasierte und angemessene Massnahmen zu überprüfen (zB durch Einholen einer Passkopie). Im Falle eines geringen Risikos kann auf die Einholung von beweiskräftigen Dokumenten im Sinne von Art 7 SPV verzichtet werden. Die Dokumentation ist zu datieren. Zu beachten ist, dass es sich bei der wirtschaftlich berechtigten Person zwingend um eine natürliche Person handelt.

Grundsätzlich ist **wirtschaftlich berechtigt**, auf dessen Veranlassung oder in dessen Interesse eine Transaktion oder Tätigkeit ausgeführt oder eine Geschäftsbeziehung letztlich begründet wird. Im Fall eines Rechtsträgers ist dies auch die natürliche Person, in deren Eigentum oder unter deren Kontrolle der Rechtsträger letztlich steht (Art 2 Abs 1 Bst e SPG; vgl idZ Art 3 SPV).

Ergänzend zur Feststellung und Überprüfung der Identität der wirtschaftlich berechtigten Person haben sich VT-Dienstleister in einem **zweiten Schritt** durch **risikobasierte** und angemessene **Massnahmen** davon zu überzeugen, dass diese Person **tatsächlich die wirtschaftlich berechtigte Person** ist. In diesem Zusammenhang ist der Fokus somit nicht auf die Identität als solche, sondern auf die Überprüfung der wirtschaftlichen Berechtigung gerichtet. Im Fall von Rechtsträgern schliesst dies risikobasierte und angemessene Massnahmen zur Feststellung der Eigentums- und Kontrollstruktur ein.

Das **Risiko**, das mit einer **Geschäftsbeziehung** oder Transaktion verknüpft ist, bestimmt dabei das **Ausmass der Überprüfung** der wirtschaftlichen Berechtigung. So ist es bei Geschäftsbeziehungen und Transaktionen mit geringen Risiken in der Regel ausreichend, wenn die Angaben zur wirtschaftlich berechtigten Person mittels einer **schriftlichen Erklärung** des Vertragspartners durch Unterschrift bestätigt werden (Art 11 Abs 2 SPV). Werden normale, erhöhte oder hohe Risiken festgestellt (s auch Anhang 3 Kapitel E SPV), bedarf es neben der schriftlichen Bestätigung nach Art 11 SPV jedenfalls weiterer Massnahmen zur Überprüfung der wirtschaftlichen Berechtigung. Hierzu zählen zB das Einholen von oder die Einsichtnahme in beweiskräftige und aktuelle Dokumente, die geeignete Informationen zur Überprüfung der wirtschaftlichen Berechtigung enthalten wie beispielsweise Beistatuten, andere Dokumente zur Begünstigtenregelung, Einkommensnachweise, Steuererklärungen oder Schenkungsverträge. Alternativ, wie auch ergänzend kann auch eine entsprechende eigene

eigenständig) die Vorteile eines VT-Systems deutlich übersteigen.

Recherche in öffentlich verfügbaren Quellen erfolgen. In welchem Umfang eine solche Recherche sinnvoll und ausreichend ist, hängt vom Risiko der jeweiligen Geschäftsbeziehung ab.

Entscheidend ist, dass VT-Dienstleister **keine Zweifel** hinsichtlich der Identität der wirtschaftlich berechtigten Personen und deren tatsächlichen wirtschaftlichen Berechtigung haben und die Ergebnisse ihrer Überprüfung plausibel sind bzw vollständig dokumentiert werden. VT-Systeme, die eine anonyme Nutzung erlauben (vgl Anhang 3 Kapitel E Ziff 1 SPV), dürften im Lichte des TVTG somit faktisch keine Rolle spielen, ausgenommen die Sorgfaltspflichtigen erfüllen ihre Verpflichtungen ergänzend ausserhalb des Systems, womit wiederum der Vorteil der Anonymität im System weitgehend wegfällt.

Jegliche Dokumente bzw Rechercheergebnisse, welche der Plausibilisierung dienen, sind daher zum Sorgfaltspflichtakt zu nehmen. Gesellschaftsrechtliche Dokumente dürfen ausnahmsweise auch ausserhalb der Sorgfaltspflichtakten dokumentiert werden.

Hinsichtlich der **Vollständigkeit der Dokumentation** in den Sorgfaltspflichtakten gelten auch hier die Vorgaben betreffend die Feststellung und Überprüfung des Vertragspartners sinngemäss. Dabei muss auch bei der Identifizierung der wirtschaftlich berechtigten Person für einen externen Dritten erkennbar sein, welche natürliche Person die Dokumentation unterzeichnet hat. Zur Feststellung der wirtschaftlich berechtigten Person und der Ausschüttungsempfänger sind die Formulare in Anhang 1 und 2 der SPV (Formular C, T und D) zu verwenden.

C. Geschäftsprofil (Art 8 SPG; Art 20 SPV)

Das Geschäftsprofil stellt die Basis für die **laufende Überwachung** einer **Geschäftsbeziehung** dar und muss dementsprechend ausreichend Informationen enthalten, um eine angemessene Überwachung durch den VT-Dienstleister sicherstellen zu können. Das Geschäftsprofil hat daher mindestens die erforderlichen **Angaben gemäss Art 20 SPV** zu enthalten und muss den individuellen Gegebenheiten und Risiken einer Geschäftsbeziehung Rechnung tragen. Die Programmierung des VT-Systems kann hierbei dienlich sein, insb bezogen auf das Transaktionsverhalten des Nutzers (vgl Anhang 3 Kapitel E Ziff 2–10 SPV) oder sonstiger für das Profil relevante Sachverhalte (vgl Anhang 3 Kapitel E Ziff 17 f SPV).

Der jeweilige Detaillierungsgrad des Profils ist abhängig von der individuellen Risikoeinstufung der Geschäftsbeziehung. Das bedeutet, je höher das Risiko einer Geschäftsbeziehung eingestuft wird, desto mehr Informationen müssen zur Geschäftsbeziehung vorliegen.

In jedem Fall – unabhängig vom konkreten, mit einer Geschäftsbeziehung verknüpften Risiko – müssen

VT-Dienstleister aufgrund der vorliegenden Informationen in der Lage sein, **Abweichungen** bzw Auffälligkeiten gegenüber den bisherigen Erfahrungen mit dem Kunden und dessen Geschäftsbeziehung, unter anderem auch durch Zugriff auf VT-systemweite Auswertungen (zB Transaktionsverhalten, Änderung der Kontaktdaten, usw) zu **erkennen**. Hierbei spielt insbesondere die konkrete Beschreibung der wirtschaftlichen Hintergründe der Geschäftsbeziehung sowie der Herkunft der eingebrachten Vermögenswerte eine zentrale Rolle. Nur durch ein vollständiges Bild über die Hintergründe zur Geschäftsbeziehung werden VT-Dienstleister in die Lage versetzt, Zusammenhänge mit Geldwäsche, Vortaten zur Geldwäsche, organisierter Kriminalität oder Terrorismusfinanzierung zu erkennen (s die Beispiele in Anhang 3 Kapitel E SPV). Zudem muss das Geschäftsprofil aussagekräftig genug sein, sodass fachkundige Dritte – beispielsweise im Rahmen einer Sorgfaltspflichtkontrolle – in der Lage sind, nach blosser Konsultation des Geschäftsprofils, ebenfalls Auffälligkeiten im Zusammenhang mit erfolgten Transaktionen etc zu erkennen.

Das Geschäftsprofil muss die VT-Dienstleister in die Lage versetzen, Abweichungen bzw Auffälligkeiten gegenüber den bisherigen Erfahrungen mit dem Kunden zu erkennen. Lässt sich beispielsweise aufgrund von zu generischen Angaben im Profil jede erdenkliche Transaktion unter ein Geschäftsprofil subsumieren, ist dieses nicht ausreichend detailliert (FMA-BK 2015/7, 161). Dies ist beispielsweise dann der Fall, wenn ein äusserst unbestimmter Betrag (zB CHF 50.000 bis CHF 1 Mio bzw Umrechnungskurs eines gehandelten Token) hinsichtlich der Vermögensein-/ausgänge angegeben wird. Grundsätzlich kann die Angabe einer gewissen Bandbreite möglich und sinnvoll sein, sofern das Profil im Kontext über genügend Aussagekraft verfügt. Folglich bedarf die angegebene Bandbreite einer gewissen Aussagekraft. Zentral ist in jedem Fall, dass die erwarteten Ein- bzw Ausgänge mit dem wirtschaftlichen Hintergrund des Vermögenseinbringers und den Angaben im Profil vereinbar sind. So wäre auch das »Mining« eines Tokens durch den Kunden lückenlos nachzuweisen, andernfalls der VT-Dienstleister nicht von einem vollständigen Profil ausgehen dürfte. Ebenfalls zu unbestimmt sind zu pauschale Angaben im Zusammenhang mit dem Verwendungszweck ohne weitere Informationen (zB »Ausgaben«, »VT-Dienstleistungen«).

Ebenfalls als ungenügend erachtet werden Angaben hinsichtlich der Herkunft der Vermögenswerte mit fehlender Aussagekraft. So reicht es beispielsweise nicht aus, wenn lediglich angegeben wird, dass die Vermögenswerte durch »Geschäftstätigkeit« erwirtschaftet wurden, ohne dass nähere Angaben zu dieser Geschäftstätigkeit vorhanden sind (s oben zum »Mining«). Auch die blosser

Angabe, der Kunde sei »Frührentner«, ohne dass weitere Informationen zur Herkunft der Vermögenswerte (beispielsweise durch langjährige Geschäftsbeziehung, die bereits vor der Pensionierung aufgenommen wurde) vorliegen, wird als nicht ausreichend erachtet.

Massgebend ist im Einzelfall der Umfang der vorhandenen Informationen. Das Profil ist generell mit zunehmendem Risiko der Geschäftsbeziehung detaillierter auszugestalten. Insbesondere in Fällen von erhöhtem Risiko (zB wenn der Nutzer mehrere Accounts innerhalb eines kurzen Zeitraums eröffnet, um Schwellenwerte zu umgehen) kann nicht darauf verzichtet werden, die Angaben des Kunden im Geschäftsprofil weiter zu plausibilisieren, beispielsweise durch die Einholung von (Dritt-) Belegen.

Konkrete Formvorgaben hinsichtlich der **Erstellung des Geschäftsprofils** und seines Umfanges sind **im SPG/in der SPV nicht enthalten**; auch die 4. GW-RL schweigt dazu. Jedoch verlangt die ratio legis, dass VT-Dienstleister **sämtliche relevanten Informationen** sammeln und zusammenhängend in den Sorgfaltspflichtakten dokumentieren. Es genügt nicht, wenn die relevanten Angaben in verschiedenen Dokumenten »auffindbar« sind; vielmehr muss das Geschäftsprofil in einer für die laufende Überwachung tauglichen sowie für Dritte verständlichen Art und Weise aufbereitet sein (es muss daher »auf Knopfdruck verfügbar sein«; vgl sinngemäss Beschluss der FMA-BK 2014/2, 6). Dieser Grundsatz gilt auch, wenn das Geschäftsprofil elektronisch, etwa über das VT-System (zentral oder dezentral) geführt wird. Die notwendigen Informationen können jedoch auch aus anderen Anwendungen oder Datenbanken an einem zentralen Ort zusammengeführt werden.

Weiters muss das **Geschäftsprofil vollständig, datiert und unterschrieben** und der Ersteller des Geschäftsprofils für einen externen Dritten erkennbar sein (vgl FMA-BK 2015/7, 16). Die Ausführungen zur Unterzeichnung der Dokumentation bei der Identifizierung des Vertragspartners gelten hier sinngemäss.

Im Fall von Mandatsübernahmen aber auch Fusionen, Übernahmen, oä Umstände, bei denen Geschäftsbeziehungen auf einen neuen Sorgfaltspflichtigen übergehen, ist es zulässig, dass das bisherige Geschäftsprofil weiterverwendet wird, wenn es den sorgfaltspflichtrechtlichen Bestimmungen entspricht, überprüft und (neu) datiert und unterschrieben wurde (vgl FMA-BK 2015/1, 5).

Das Geschäftsprofil ist stets **aktuell** zu halten. VT-Dienstleister haben die Unterlagen und Akten in regelmässigen Abständen aktiv von sich aus (dh beispielsweise durch Kontaktaufnahme mit dem Vertragspartner, Einholen entsprechender Unterlagen, eigener Recherche, Aufnahme neuer Sachverhalte) durch den Sorgfaltspflichtigen zu überprüfen und ggfalls aktualisieren.

D. Risikoadäquate Überwachung von Geschäftsbeziehungen (Art 9–9b SPG; Art 22 SPV)

Gemäss Art 9 Abs 1 SPG haben VT-Dienstleister eine **zeitnahe risikoadäquate Überwachung ihrer Geschäftsbeziehungen**, einschliesslich der im Verlauf der Geschäftsbeziehung abgewickelten Transaktionen, durchzuführen, um sicherzustellen, dass diese mit dem Geschäftsprofil (Art 8 SPG) übereinstimmen.

Der Prozess für die Überwachung der Geschäftsbeziehung ist angemessen in den internen Weisungen bzw der Risikobewertung nach Art 9a SPG zu regeln und den betroffenen Beschäftigten für die tägliche Anwendung zur Kenntnis zu bringen.

Registrierungspflichtige VT-Dienstleister sind verpflichtet, unter Berücksichtigung des Stands der Technik informatikgestützte Systeme einzusetzen, um risikobasiert die Historie der entsprechenden virtuellen Währungen bzw Token in ihrem VT-System (Art 2 Abs 1 Bst b TVTG) zu überprüfen (Art 9b Abs 2 SPG). In der Praxis dürfte die umfassende und lückenlose Möglichkeit zum Monitoring der Token im VT-System eine ungeschriebene Vorbedingung für VT-Dienstleister sein, da diese ohne dieses Instrument ihre Sorgfaltspflichten kaum effektiv erfüllen könnten.

Die **Transaktionsüberwachung** hat entsprechend den gesetzlichen Vorgaben zeitnah, sprich ohne Verzögerung nach Erhalt der Transaktionsbelege oder ab Kenntnis der Transaktion zu erfolgen. Dabei hat nach Erhalt der Transaktionsbelege (Tages-, Monats- oder Quartalsauszüge; im VT-System womöglich sogar hochfrequenter) oder Kenntnis der Transaktion ein Abgleich mit dem jeweiligen Geschäftsprofil stattzufinden, um die Profilkonformität festzustellen. Dieser Abgleich hat bei Geschäftsbeziehungen mit erhöhten oder hohen Risiken nachweislich binnen 14 Tagen ab Erhalt der Transaktionsbelege oder ab Kenntnis der Transaktion zu erfolgen.¹⁶

In den übrigen Fällen, dh bei Geschäftsbeziehungen mit einem normalen oder geringen Risiko wird eine Frist von grundsätzlich 30 Tagen für den Abgleich einer Transaktion mit dem Profil als angemessen erachtet. Sonderregeln bestehen für VT-Systeme und VT-Dienstleister nicht.

Sollte eine Transaktion nicht dem Geschäftsprofil entsprechen, haben VT-Dienstleister in weiterer Folge mit der Durchführung einer einfachen oder gegebenenfalls einer besonderen **Abklärung** (Art 9 SPG; Art 22 SPV) vorzugehen. Ergänzend ist zu erwähnen, dass Bargeldtransaktionen, zB bei Wechsel von Bargeld in Token, aus Sicht der Geldwäschereibekämpfung ein höheres Risiko als Transaktionen mittels Banküberweisung darstellen.

Dem Risiko dieser Geschäfte ist dahingehend Rechnung zu tragen, dass bei Bartransaktionen jeweils zum Durchführungszeitpunkt mit der Plausibilisierung begonnen werden muss, sofern diese nicht ohnehin schon dem Profil entsprechen (zB Einzahlung kleiner Teile der Tageslosungen von Klein- und Mittelbetrieben zur Vermögensdiversifizierung und/oder Spekulation auf eigene Rechnung). Eine nachgelagerte Überwachung macht grundsätzlich nur wenig Sinn und genügt folglich bei der Durchführung von Bartransaktionen den Anforderungen des SPG und der SPV nicht. Dieses Erfordernis ist zudem durch den Umstand gerechtfertigt, dass sich der Kunde zur Durchführung von Bartransaktionen regelmässig bereits im jeweiligen Institut bzw beim jeweiligen Dienstleister befindet.

Als Folge der risikoadäquaten Überwachung haben VT-Dienstleister nach Art 9 Abs 3 SPG mit angemessenem Aufwand **einfache Abklärungen** zu tätigen, sofern Sachverhalte oder Transaktionen auftreten, die vom Geschäftsprofil abweichen. VT-Dienstleister sollen nach Art 22 Abs 1 SPV in diesem Zusammenhang die Informationen beschaffen, auswerten und dokumentieren, die geeignet sind, den Hintergrund solcher Sachverhalte oder Transaktionen nachvollziehbar und verständlich zu machen.

Nach Art 9 Abs 4 SPG sind **besondere Abklärungen** zu tätigen, wenn Sachverhalte oder Transaktionen auftreten, die Verdachtsmomente in Richtung Geldwäscherei, Vortaten der Geldwäscherei, organisierter Kriminalität oder Terrorismusfinanzierung begründen. Anlass zu solchen Abklärungen können unter anderem auch die Anhaltspunkte für Geldwäscherei, organisierte Kriminalität und Terrorismusfinanzierung, welche im Anhang 3 der SPV aufgelistet sind, geben. Während der Durchführung dieser Abklärungen dürfen VT-Dienstleister die **Geschäftsbeziehung nicht abbrechen**. In diesem Zusammenhang ist allenfalls Art 18 SPG zu beachten. Nach Art 22 Abs 2 SPV haben VT-Dienstleister im Rahmen von besonderen Abklärungen die Informationen zu beschaffen, auszuwerten und zu dokumentieren, die geeignet sind, allfällige Verdachtsmomente nach Art 17 Abs 1 SPG auszuräumen oder zu erhärten.

Um **Abweichungen vom Geschäftsprofil** oder Verdachtsmomente **auszuräumen**, müssen VT-Dienstleister geeignete Informationen im Sinne von Art 22 SPV beschaffen, damit die betreffenden **Sachverhalte** oder Transaktionen **plausibilisiert** werden können. VT-Dienstleister müssen im Ergebnis darauf vertrauen können, dass keine ungeklärten Sachverhalte oder Verdachtsmomente (mehr) vorliegen. In diesem Zusammenhang ist zu beachten, dass Verdachtsmomente in Richtung Geldwäscherei oder Vortaten zur Geldwäscherei nicht erst dann entstehen, wenn VT-Dienstleister Kenntnis von einer konkreten Vortat oder des tatsächlichen

¹⁶ BuA 2016/159, 67 (SPG).

Täters der Vortat hat. Nach StGH 2014/152, Erw 8.4., sei es für die Verwirklichung des Tatbestandes der Geldwäscherei (§ 165 StGB) nicht notwendig, dass die Vortat, aus welcher die inkriminierten Vermögensbestandteile stammen, nach Ort, Zeit, Täter, Tatmodalität etc erwiesen ist oder gar in einem schuldig sprechenden Urteil festgestellt wird oder wurde. Umso mehr muss dies auf der Ebene der besonderen Abklärungen gelten, welche bereits durch blosse Verdachtsmomente ausgelöst werden.¹⁷

Erklärungen des Kunden im Rahmen einer spezifischen Transaktionsabklärung sind auf ihre Plausibilität hin zu überprüfen. Wichtig ist, dass nicht jede Erklärung des Kunden pauschal und ungeprüft akzeptiert werden kann. Abhängig vom jeweiligen Risiko sind demnach (Dritt-) Belege zwecks Plausibilisierung von Erklärungen einzuholen.

Die **Resultate** aus den **Abklärungen** sind nach Art 9 Abs 5 SPG in den **Sorgfaltspflichtakten** zu **dokumentieren**. Der Zeitraum für die Durchführung einer einfachen oder besonderen Abklärung ist anhand des Risikos der jeweiligen Geschäftsbeziehung bzw des Gewichts des Verdachtsmomentes zu bestimmen. Eine klare Fristvorgabe ist daher im Gesetz nicht enthalten. Es gilt jedoch die »Faustregel«, je ungewöhnlicher und riskanter ein VT-Dienstleister eine Transaktion oder einen Sachverhalt einstuft (s hierzu Anhang 3 Kapitel E SPV), desto schneller sollte er die erforderlichen Abklärungen durchführen. Abklärungen nach Art 9 Abs 4 SPG dürfen daher nicht Monate andauern.¹⁸ Zu bedenken ist idZ, dass VT-Dienstleister ggfalls auch zur Erstattung einer Verdachtsmeldung gemäss Art 17 SPG verpflichtet sein könnten.

E. Abgleich hinsichtlich politisch exponierter Personen (PEP) (Art 11 Abs 4 SPG)

VT-Dienstleister sind zudem verpflichtet, Abklärungen hinsichtlich PEP durchzuführen. Gemäss Art 2 Abs 1 Bst h SPG handelt es sich bei einer »Politisch Exponierten Person« (PEP) um eine natürliche Person, die wichtige öffentliche Ämter ausübt oder bis vor einem Jahr ausgeübt hat. Dabei gilt als PEP nur eine Person, die auf staatlicher Ebene Funktionen wahrnimmt. Als PEP gelten daher Richter höherer Gerichte, deren Entscheidungen nicht mehr anfechtbar sind (zB StGH), Mitglieder von (Landes)parlamenten, Bürgermeister, Honorarkonsule oÄ (vgl auch Art 2 SPV).

VT-Dienstleister haben bei Aufnahme einer Geschäftsbeziehung oder Abwicklung einer gelegentlichen

Transaktion mit einer PEP zu überprüfen, ob es sich beim Vertragspartner oder bei der wirtschaftlich berechtigten Person um eine PEP handelt oder nicht (sog »PEP-Abgleich«).

Dieser Verpflichtung haben VT-Dienstleister **unverzüglich**, nämlich sofort bei Aufnahme der Geschäftsbeziehung oder Abwicklung der gelegentlichen Transaktion zu entsprechen (FMA-BK 2015/1, 5). Nur so kann nämlich den Verpflichtungen nach Art 11 SPG nachgekommen werden, wenn festgestellt wird, ob eine Geschäftsbeziehung oder gelegentliche Transaktionen mit einer PEP überhaupt bestehen.

Darüber hinaus haben VT-Dienstleister einen regelmässigen **PEP-Abgleich** des gesamten Kundenstamms zu gewährleisten, um im Rahmen von bestehenden Geschäftsbeziehungen die Identifikation von PEP sicherzustellen. Dieser regelmässige PEP-Abgleich hat mindestens jährlich zu geschehen. Der PEP-Abgleich bezieht sich auch auf den Ausschüttungsempfänger nach Art 2 Abs 1 Bst p SPG.

Grundsätzlich hat der PEP-Abgleich jeweils im Zeitpunkt der Auszahlung der Ausschüttung zu erfolgen. VT-Dienstleister, die gemäss Art 7a Abs 3 SPG über die Identität des Ausschüttungsempfängers von anderen Sorgfaltspflichtigen verständigt werden, müssen allerdings erst nach erfolgter Verständigung einen PEP-Abgleich durchführen.

Sowohl der PEP-Abgleich (einschliesslich der »Negativ-Treffer«) als auch die Zustimmung mindestens eines Mitglieds der Leitungsebene über die Aufnahme bzw Weiterführung von Geschäftsbeziehungen mit PEP müssen im Sorgfaltspflichtakt dokumentiert sein (FMA-BK 2015/1, 5).

Bei VT-Dienstleistern, die ein **automatisiertes, informatikgestütztes System** zur Ermittlung von Geschäftsbeziehungen und Transaktionen mit PEP einsetzen (Art 21 Abs 1 SPV), kann die Dokumentation der Negativ-Treffer des erfolgten PEP-Abgleichs ausnahmsweise an einem zentralen Ort (physisch oder elektronisch) erfolgen. In solch einem Fall müssen VT-Dienstleister die Zuordnung des PEP-Abgleichs zu den jeweiligen Sorgfaltspflichtakten sicherstellen. Auf Verlangen muss der Nachweis des erfolgten PEP-Abgleichs für bestimmte Personen unverzüglich (ohne unnötigen Aufschub) erfolgen, sohin der Negativ-Treffer direkt vorgelegt werden können. Die Positiv-Treffer sind demgemäss im Sorgfaltspflichtakt zu dokumentieren.

VT-Dienstleister haben ab einer Gesamtzahl von 100 verwalteten Geschäftsbeziehungen verpflichtend ein automatisiertes, informatikgestütztes System (zB World-Check) zur Ermittlung von Geschäftsbeziehungen und Transaktionen mit PEP zu verwenden (Art 21 Abs 1 SPV). Eine Verknüpfung des VT-Systems mit spezialisierten externen Anbietern erscheint hier zulässig und sinnvoll.

17 Vgl auch *Schmidle*, Neues zur Geldwäscherei aus Wien und Strassburg, LJZ 2018, 78 ff.

18 Landgericht 3.12.2018, 13 EU.2018.142 Rn 54.

F. Zeitpunkt der Wahrnehmung der Sorgfaltspflichten

Vgl zu Beginn der Sorgfaltspflichten oben VII.A. Die zuvor skizzierten Sorgfaltspflichten sind jeweils in den Fällen des Art 5 Abs 2 SPG vorzunehmen, somit ua bei **Aufnahme einer Geschäftsbeziehung** oder bei **Abwicklung gelegentlicher Transaktionen**.

Eine Geschäftsbeziehung gilt dann als aufgenommen, wenn sorgfaltspflichtrechtlich relevante Tätigkeiten ausgeübt werden (hier gem Art 3 Abs 1 Bst r-t SPG), zB durch Anlegen von Neu-Kundendossiers durch Betreiber von Handelsplattformen oder Bündelung der konkreten Angebote kurz vor Vollziehung der Token-Emission.

An dieser Stelle ist nochmals hervorzuheben, dass für registrierungspflichtige VT-Dienstleister (Art 3 Abs 1 Bst r SPG) idZ keine Schwellenwertgrenzen (etwa bei gelegentlichen Transaktionen) gelten (Art 5 Abs 2 Bst g SPG; anderes gilt für VT-Wechseldienstleister gem Art 5 Abs 2 Bst h SPG).

Können die Sorgfaltspflichten nicht wahrgenommen werden, dürfen VT-Dienstleister die **Geschäftsbeziehung nicht aufnehmen** bzw **fortführen** und die gewünschte **Transaktion nicht durchführen**. VT-Dienstleister müssen prüfen, ob eine Mitteilung nach Art 17 SPG an die SFIU notwendig ist. Ebenso ist eine **bestehende Geschäftsbeziehung abubrechen**, wenn die Sorgfaltspflichten nicht wahrgenommen werden können. Der Abbruch hat hier unter hinreichender Dokumentation des Abflusses der Vermögenswerte zu erfolgen. Allfällige Mitteilungspflichten nach Art 17–19 SPG bleiben unberührt. Der Abbruch einer bestehenden Geschäftsbeziehung hat Vorrang gegenüber anderen gesetzlichen oder vertraglichen Bestimmungen (Art 5 Abs 3 Bst b SPG) wie auch VT-Systemen internen Reglementen und/oder Mechanismen. Der Programmcode eines VT-System hat den jederzeitigen Abbruch einer Geschäftsbeziehung somit jederzeit zu ermöglichen, andernfalls die Sicherstellung der Sorgfaltspflichten durch den VT-Dienstleister nicht gewährleistet werden kann.

Haben VT-Dienstleister **Zweifel an der Identität des Vertragspartners** oder der wirtschaftlich berechtigten Person, so haben sie die **Identifikation zu wiederholen**. Bestehen danach weiterhin Zweifel, aber noch kein Verdacht iSv Art 17 SPG (vgl ansonsten zum weiteren Vorgehen Art 15 Abs 2 SPV) und brechen sie deswegen die Geschäftsbeziehung ab, dürfen sie den Rückzug der Vermögenswerte (Token) nur unter hinreichender Dokumentation des Abflusses der Vermögenswerte zulassen. Dies erlaubt den zuständigen Behörden, nötigenfalls die Spur weiterzuverfolgen, womöglich unter Nutzung der internen Dokumentation des VT-Dienstleisters oder des VT-Systems. VT-Dienstleister dürfen in einem

solchen Fall Gelder nicht bar auszahlen, Titel und Edelmetalle physisch herausgeben oder Token per VT-System rückvergüten, es sei denn, der Vertragspartner ist seinen Pflichten vollumfänglich nachgekommen und die Dokumentation ist vollständig.

Art 18 Abs 2 SPV bestimmt in diesem Zusammenhang, dass in Fällen, in denen dies für die Aufrechterhaltung des normalen Geschäftsverkehrs notwendig ist und ein geringes Risiko für Geldwäscherei und Terrorismusfinanzierung nach Art 10 SPG festgestellt wurde, die Überprüfung der Identität des Vertragspartners oder der wirtschaftlich berechtigten Person sobald wie möglich nach dem ersten Kontakt durchzuführen und sicherzustellen ist, dass in der Zwischenzeit keine Vermögensabflüsse stattfinden.

In jedem Fall ist eine **Einzelfallbeurteilung** vorzunehmen. Ohne Vorliegen der erforderlichen Dokumente dürfen jedenfalls keine Vermögenswerte (Token) abfließen. Was als »normaler Geschäftsverkehr« im Sinne des Art 18 Abs 2 SPV zu betrachten ist, richtet sich nach dem Einzelfall. Kein »normaler Geschäftsverkehr« liegt beispielsweise vor, wenn Zweifel bezüglich der Angaben des Vertragspartners zur wirtschaftlich berechtigten Person oder zum Geschäftsprofil vorliegen.

G. Mitteilungspflicht an die SFIU

Ergibt sich nach den getätigten Abklärungen der **Verdacht auf Geldwäscherei**, eine Vortat der Geldwäscherei, organisierte Kriminalität oder Terrorismusfinanzierung, haben VT-Dienstleister nach Art 17 Abs 1 SPG der Stabsstelle FIU umgehend schriftlich Anzeige zu erstatten. Die Verantwortung für die Erstattung der Mitteilung obliegt dabei dem für die Einhaltung des SPG bestimmten (verantwortlichen) Mitglieds der Geschäftsleitung des VT-Dienstleisters. Näheres dazu unter in der Wegleitung der SFIU zur Erstattung von Verdachtsmitteilungen gemäss Art 17 SPG.¹⁹

H. Dokumentation (Art 20 SPG; Art 27 ff SPV)

Gemäss Art 20 Abs 1 SPG müssen VT-Dienstleister die **Einhaltung der Sorgfaltspflichten** nach Art 5–16 SPG und der Mitteilungspflicht an die SFIU nach Art 17 SPG nach Massgabe des SPG **dokumentieren**. Zu diesem Zweck müssen VT-Dienstleister **Sorgfaltspflichtakten** führen und diese aufbewahren. Solange die Sorgfaltspflichtakten auch offline jederzeit zugänglich sind, dürfte auch eine Abbildung im VT-System (zB aufgrund der Möglichkeit höherfrequenter Aktualisierungen) grundsätzlich zulässig sein (s sogleich unten).

¹⁹ <<https://www.llv.li/files/sfiu/20170925-fiu-wegleitung-konsolidiert.pdf>>(gesehen am 21.7.2021).

Nach Art 27 Abs 1 SPV müssen die Akten insbesondere die zur Einhaltung des SPG und der SPV erstellten und beigezogenen Unterlagen und Belege enthalten. Neben den Dokumenten und Unterlagen, die der Feststellung und Überprüfung der Identität des Vertragspartners und der wirtschaftlich berechtigten Person gedient haben, dem Geschäftsprofil und den Transaktionsunterlagen, müssen die Sorgfaltspflichtakten auch die Dokumentation über allfällige Abklärungen nach Art 9 SPG sowie alle in diesem Zusammenhang beigezogenen Dokumente, Unterlagen und Belege enthalten. Zudem sind die Gründe für die Anwendung vereinfachter oder verstärkter Sorgfaltspflichten nach Art 10 und 11 SPG in den Sorgfaltspflichtakten zu dokumentieren. Alternativ kann die Dokumentation dieser Gründe auch in anderen geeigneten internen Dokumenten erfolgen, wie beispielsweise der Mandatsliste oder einer Risikomatrix.

Nach Art 28 Abs 1 Bst b SPV müssen die Sorgfaltspflichtakten so angelegt sein, dass sie fachkundigen Dritten ein zuverlässiges Urteil über die Einhaltung der Bestimmungen des SPG und der SPV ermöglichen. Sie können nach Art 28 Abs 2 SPV unter bestimmten Voraussetzungen schriftlich, elektronisch (s oben zur Dokumentation im VT-System) oder in vergleichbarer Weise aufbewahrt werden. Unter Verweis auf die Voraussetzungen der elektronischen Aufbewahrung in Art 28 Abs 2 SPV ist es möglich, dass die Sorgfaltspflichtakten gänzlich in elektronischer Form aufbewahrt werden, ohne dass gleichzeitig gewisse Dokumente wie beispielsweise Identifikationsdokumente physisch im Original aufbewahrt werden müssen. Diese können nach deren Digitalisierung vernichtet werden. Ergänzend sei an dieser Stelle auf Art 28 Abs 3 SPV hingewiesen, wonach die Bild- und Datenträger regelmässig auf ihre Integrität und Lesbarkeit zu prüfen sind. Im Idealfall wird demgemäss jeweils eine Sicherungskopie der elektronischen Datenträger erstellt, um damit den jederzeitigen Zugriff sicherzustellen. Darüber hinaus ist bei einer elektronischen Aufbewahrung auch zu beachten, dass die Prüfung der Aufzeichnungen nicht schwieriger sein oder mehr Zeit beanspruchen darf als die Prüfung der zugrundeliegenden Unterlagen.

Die jeweils relevanten Informationen sind gesammelt und aufbereitet in den Sorgfaltspflichtakten zu dokumentieren. Muss sich ein fachkundiger Dritter die Informationen erst einzeln zusammensuchen, würde das zu keinem zuverlässigen Urteil über die Einhaltung der Bestimmungen des SPG und der SPV führen (vgl FMA-BK 2014/2, 6).

Zusammenfassend sind die Sorgfaltspflichtakten so zu führen, dass sich eine Drittperson, die mit den Vorschriften des SPG und der SPV vertraut ist, problemlos einen Überblick über die Geschäftsbeziehung und deren Risiken verschaffen kann. Insbesondere bedeutet dies,

dass Informationen, die Beschäftigten der VT-Dienstleister aufgrund ihres persönlichen Hintergrundes geläufig sind, einerseits in den Sorgfaltspflichtakt aufzunehmen und andererseits so aufzubereiten sind, dass sie für einen externen Dritten lesbar und verständlich sind. Dies bedeutet insbesondere auch, dass die Sorgfaltspflichtakten grundsätzlich auf Deutsch zu führen sind. Basisdokumente (zB der Dossier-Eröffnungsantrag [Onboarding], Formulare zur Identifizierung von Vertragspartner und wirtschaftlich berechtigter Person) können dabei in Fremdsprachen vorhanden sein. Es ist jedoch zu beachten, dass bei Unterlagen, welche der Plausibilisierung von Informationen und Transaktionen dienen und welche vom Kunden in einer Fremdsprache, welche nicht Englisch ist, eingereicht wurden, relevante Passagen auf Deutsch oder Englisch übersetzt werden, sodass die darin getätigten Aussagen durch einen Dritten geprüft werden können. Die FMA kann bei Bedarf die Übersetzung auch englischer Dokumente in Deutsch anordnen.

Die **Aufbewahrung der Sorgfaltspflichtakten** hat an einem jederzeit zugänglichen Ort im Inland zu erfolgen (Art 28 Abs 5 SPV). Der Grund dafür besteht darin, dass der jederzeitige Zugriff der zuständigen inländischen Aufsichtsbehörden gewährleistet sein muss. Bei einer elektronischen Aufbewahrung der Sorgfaltspflichtakten ist es zwar zulässig, dass das System zur Aufbewahrung (»Server«) im Ausland geführt wird, es muss jedoch sichergestellt sein, dass die Daten der Sorgfaltspflichtakten jederzeit in aktueller Form im Inland verfügbar sind. Dies kann beispielsweise durch eine regelmässige Synchronisation und Speicherung der Daten im Inland erfolgen, wie auch durch die Mehrfachkopierung auf dezentralen Hauptbüchern.

I. Interne Organisation (Art 21 SPG; Art 31 ff SPV)

VT-Dienstleister müssen die nach Gesetz bzw SPV erforderlichen **organisatorischen Massnahmen** implementieren und für geeignete interne Kontroll- und Überwachungsmassnahmen sorgen (**Einrichtung eines IKS**). VT-Dienstleister haben idZ insbesondere interne Weisungen zu erlassen, die sichere Aufbewahrung der Sorgfaltspflichtakten zu veranlassen und für die Aus- und Weiterbildung ihres Personals Sorge zu tragen.

Die interne Organisation muss den Umständen und den individuellen Risiken entsprechend je nach Art und Grösse des VT-Dienstleisters sowie nach Anzahl, Art und Komplexität der Geschäftsbeziehungen ausgestaltet sein. Die wirkungsvolle Wahrnehmung der internen Funktionen sowie der Sorgfaltspflichten muss stets gewährleistet sein.

►

1. Interne Weisungen (Art 21 Abs 1 SPG; Art 31 SPV)

VT-Dienstleister haben interne Weisungen zu erstellen, welche mindestens die Angaben nach Art 31 SPV enthalten. Sie haben in ihrer Ausgestaltung der Art und Komplexität der Geschäftstätigkeit des VT-Dienstleisters Rechnung zu tragen. Die internen Weisungen sind allen an Geschäftsbeziehungen mitwirkenden Beschäftigten zur Kenntnis zu bringen und durch die Geschäftsleitung zu erlassen.

Die Weisungen sind derart auszugestalten, dass sie den Beschäftigten des Unternehmens als Leitfaden in der Wahrnehmung der Sorgfaltspflichten dienen können. Entsprechend reicht es in der Regel nicht, wenn in den Weisungen lediglich der Gesetzes- bzw Verordnungstext wiedergegeben wird. Vielmehr haben VT-Dienstleister die internen Weisungen spezifisch für ihre Geschäftstätigkeit, inklusive konkreter operativer Prüfschritte, auszuformulieren.

2. Aus- und Weiterbildung (Art 21 Abs 1 SPG; Art 32 SPV)

VT-Dienstleister haben für eine aktuelle und umfassende **Aus- und Weiterbildung** ihrer Beschäftigten, die an Geschäftsbeziehungen mitwirken, zu sorgen. Dabei müssen Kenntnisse über die Vorschriften zur Verhinderung und Bekämpfung von Geldwäscherei, Vortaten der Geldwäscherei, organisierter Kriminalität und Terrorismusfinanzierung sowie über das Datenschutzrecht vermittelt werden. Es sind zumindest, neben dem grundlegenden Wissen über VT-Systeme, die nachfolgenden Themen abzudecken:

- die sich aus dem SPG und der SPV ergebenden Pflichten;
- die massgeblichen Bestimmungen des StGB;²⁰
- die internen Weisungen;
- das Vermitteln von Kenntnissen, die es den Beschäftigten ermöglichen, Transaktionen, die möglicherweise mit Geldwäscherei, organisierter Kriminalität oder Terrorismusfinanzierung zusammenhängen, zu erkennen und sich in solchen Fällen richtig zu verhalten;
- die massgeblichen Bestimmungen des DSGVO²¹ und der EU-DSGVO.²²

²⁰ Strafgesetzbuch (StGB) vom 24. Juni 1987, LGBl 1988.37.

²¹ Datenschutzgesetz (DSG) vom 4. Oktober 2018, LGBl 2018.272.

²² Verordnung (EU) 2016/679 DES Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl 2016 L 119, 1, idF der Berichtigung, ABl 2018 L 127, 2.

Idealerweise werden von VT-Dienstleistern und ihren Beschäftigten externe Aus- und Weiterbildungsveranstaltungen besucht. Dabei ist es selbstverständlich zulässig, dass im Rahmen von internen Schulungen die Inhalte auch von externen Veranstaltungen in der Folge weitergegeben werden.

3. Interne Funktionen (Art 22 SPG; Art 33 ff SPV)

VT-Dienstleister müssen eine Ansprechperson für die FMA als zuständige Aufsichtsbehörde (Art 23 SPG) sowie Personen oder Fachstellen für die internen Funktionen Sorgfaltspflichtbeauftragter und Untersuchungsbeauftragter benennen.

Zudem muss ein Mitglied der Geschäftsleitung oder »in vergleichbarer Person« (Art 2 Abs 1 Bst r SPG) bestimmt werden, welches für die Einhaltung des Sorgfaltspflichtenrechts gegenüber der FMA verantwortlich ist. Zielsetzung dieser Regelung ist es, ein möglichst starkes »Commitment« für die Geldwäschereibekämpfung in den obersten Organen des VT-Dienstleisters zu generieren.

Dementsprechend versteht die FMA unter dem Begriff »**Personen in vergleichbarer Funktion**« im Sinne von Art 2 Abs 1 Bst r SPG nur solche Personen, die den Mitgliedern der Geschäftsleitung, des Verwaltungsrates etc hierarchisch gleichgestellt sind und über vergleichbare Befugnisse wie die Mitglieder der Geschäftsleitung, des Verwaltungsrates etc verfügen. Beispielsweise erfüllt ein »Head of Compliance«, der der Complianceabteilung vorsteht und über die erforderlichen ausreichenden Befugnisse verfügt, die Qualifikation des verantwortlichen Mitglieds der Leitungsebene nicht, wenn er nicht zugleich auch Mitglied der Geschäftsleitung ist. Sofern keine Geschäftsleitung existiert, erfordert es zumindest die hierarchische Gleichstellung auf Ebene des Verwaltungsrates oder eines anderen gleichwertigen Gremiums.

Das nach SPG **verantwortliche Mitglied der Leitungsebene** oder die »Person in vergleichbarer Position« muss über **fundierte Kenntnisse** in Fragen der Verhinderung und Bekämpfung von Geldwäscherei, Vortaten der Geldwäscherei, organisierter Kriminalität und Terrorismusfinanzierung und über das Datenschutzrecht verfügen sowie die aktuellen Entwicklungen in diesen Bereichen kennen. Daneben wird die Tätigkeit in einem VT-Dienstleister zumindest fundamentale Kenntnisse über die Funktionsweise von VT-Systemen verlangen. Zudem ist diese Person mit ausreichenden Befugnissen auszustatten, um die Einhaltung des Sorgfaltspflichtenrechts durch den Sorgfaltspflichtigen sicherzustellen (Art 36 Abs 1 und 2 SPV).

Verletzt das verantwortliche Mitglied der Geschäftsleitung oder die »Person in vergleichbarer Funktion«

seine/ihre **Überwachungspflichten** bzw unterlässt er/sie es, eine **adäquate Binnenorganisation** im Institut umzusetzen, kann das betreffende Mitglied der Leitungsebene verwaltungsstrafrechtlich zur Verantwortung gezogen werden (**Art 33 Abs 1 SPG**). Daher hat der VT-Dienstleister, bei sonstiger Sanktion, sicherzustellen, dass diese Person über **freien Zugang zu sämtlichen Informationen**, Daten, Aufzeichnungen und Systemen erhält, welche sie zur Erfüllung ihrer Aufgaben benötigt. Es muss ihr möglich sein, Transaktionen zu stoppen, Konten zu sperren und andere derartige Massnahmen anzuordnen. Ebenfalls muss ihr ein Vetorecht hinsichtlich der Aufnahme oder Fortführung einer Geschäftsbeziehung zustehen bzw muss sie die Beendigung einer solchen durchsetzen können. Darüber hinaus obliegt dieser Person im Sinne von Art 17 Abs 1 SPG die Verantwortung für die Erstattung einer Verdachtsmitteilung an die SFIU. Abweichungen von diesen Vorgaben können einerseits zu verwaltungsstrafrechtlichen Konsequenzen führen (Art 33 SPG); andererseits muss das verantwortliche Mitglied der Geschäftsleitung, wenn es von einem anderen Mitglied der Geschäftsleitung überstimmt (*»Overruling«*) wird oder die Einhaltung der internen Prozesse und Weisungen nicht gewährleisten kann, sein Amt bei sonstiger Sanktion zurücklegen.

Auch dem Sorgfaltspflichtbeauftragten und dem Untersuchungsbeauftragten sind zur Wahrnehmung ihrer Aufgaben jederzeit Zugang zu den Sorgfaltspflichtakten zu gewähren. Zudem müssen die genannten Funktionsträger über fundierte Kenntnisse in Fragen der Verhinderung und Bekämpfung von Geldwäscherei, Vortaten der Geldwäscherei, organisierter Kriminalität und Terrorismusfinanzierung und über das Datenschutzrecht verfügen sowie die aktuellen Entwicklungen in diesen Bereichen kennen. Wird eine Fachstelle für die Funktionen des Sorgfaltspflichtbeauftragten oder Untersuchungsbeauftragten eingesetzt, so ist zu beachten, dass die ausführenden Personen ebenso die beschriebenen sorgfaltspflichtrechtlichen Qualifikationen zu erfüllen haben. Zudem muss für einen fachkundigen Dritten im Sinne von Art 28 Abs 1 Bst b SPV jederzeit erkennbar sein, von welchen Personen die Aufgaben jeweils wahrgenommen worden sind, beispielsweise durch erkennbare Zeichnung der zu Grunde liegenden Dokumentation.

Eine Person oder gegebenenfalls Fachstelle kann mehrere Funktionen erfüllen, sofern die Umsetzung des SPG gewährleistet ist. IdZ ist zu beachten, dass die Funktionen des Sorgfaltspflichtbeauftragten und Untersuchungsbeauftragten grundsätzlich unterschiedlichen Personen zuzuteilen sind, um somit eine Aufgabentrennung sicherzustellen. Eine dieser beiden Funktionen kann auch durch das verantwortliche Mitglied der Leitungsebene wahrgenommen werden, sofern die Umsetzung des SPG gewährleistet wird. Dies bedingt unter

anderem, dass dem Mitglied der Leitungsebene ausreichend Ressourcen zur Wahrnehmung einer weiteren Funktion zur Verfügung stehen. Die darüber hinausgehende Ausübung mehrerer Funktionen (vorbehaltlich jener der Ansprechperson) durch eine einzige Person ist auf jene Fälle zu beschränken, in denen die Grösse des Sorgfaltspflichtigen eine Aufgabentrennung nicht zulässt (zB Einzelunternehmen).

Werden die Aufgaben des Sorgfaltspflichtbeauftragten oder Untersuchungsbeauftragten entsprechend qualifizierten internen oder externen Personen oder Fachstellen übertragen (**Delegation**), bleiben die **Funktionsträger für die ordnungsgemässe Wahrnehmung ihrer Funktionen verantwortlich**. Anders verhält es sich lediglich, wenn nicht nur die Aufgaben, sondern die Funktion als solche auf eine Person oder Fachstelle übertragen wird. Die Stellvertretung der internen Funktionen ist jederzeit zu gewährleisten. Dies bedeutet, dass für sämtliche der Funktionen (Ansprechperson, Sorgfaltspflichtbeauftragter, Untersuchungsbeauftragter, verantwortliches Mitglied der Leitungsebene) eine Stellvertretung mit denselben geforderten fachlichen und hierarchischen Qualifikationen zu bestimmen ist. Betreffend das verantwortliche Mitglied der Leitungsebene kann ausnahmsweise auf die Bestimmung einer Stellvertretung verzichtet werden, sofern aufgrund der Grösse des Sorgfaltspflichtigen keine weitere qualifizierte Person zur Verfügung steht (zB Einzelunternehmen). Sofern es die Grösse des Sorgfaltspflichtigen zulässt, hat der Sorgfaltspflichtige jedoch dafür Sorge zu tragen, dass die erforderlichen Qualifikationen von einem vorhandenen Mitglied der Leitungsebene als Stellvertreter erfüllt werden (zB durch entsprechende Schulungen). Ungeachtet der Ausnahme ist jedoch bei einer voraussehbaren längeren Abwesenheit (zB medizinische Behandlungen, Sonderurlaube) ein neues verantwortliches Mitglied der Leitungsebene im Sinne des Sorgfaltspflichtrechts für die Dauer der Abwesenheit zu bestimmen. In einem solchen Fall genügt es, wenn diese Person mit den ausreichenden Befugnissen im Sinne von Art 36 Abs 2 SPV ausgestattet ist, die Bestellung als Organ des Rechtsträgers ist hingegen nicht zwingend erforderlich.

VT-Dienstleister haben die Einsetzung und den Wechsel der Funktionsträger sind der FMA spätestens binnen fünf Werktagen nach Aufnahme der Funktion mitzuteilen (vgl dazu FMA-Wegleitung 2020/1, Anhang 6).

J. Sorgfaltspflichtkontrollen

VT-Dienstleister werden in regelmässigen Abständen durch von der FMA beauftragte Wirtschaftsprüfer und Revisionsgesellschaften auf die Einhaltung des SPG und der SPV sowie der durch die FMA erlassenen Richtlinien,

Mitteilungen und Wegleitungen geprüft (ordentliche Sorgfaltspflichtenkontrollen). Dabei wird grundsätzlich der in Art 37a Abs 1 SPV festgelegte Prüfrhythmus angewandt. Die FMA kann in Ausnahmefällen von diesem festgelegten Prüfrhythmus abweichen.

Bei Zweifel über die Wahrnehmung von Sorgfaltspflichten oder bei Vorliegen von Umständen, die den Ruf des Finanzplatzes als gefährdet erscheinen lassen, führt die FMA darüber hinaus ausserordentliche Kontrollen durch bzw lässt diese durchführen (vgl dazu FMA-Richtlinie 2013/2).

VIII. Risikomatrix nach SPG

Vgl dazu FMA-Richtlinie 2013/1 zum SPG. VT-Dienstleister sind als Sorgfaltspflichtige aufgrund ihrer Tätigkeit einem erheblichen Risiko ausgesetzt, für Zwecke der Geldwäscherei oder Terrorismusfinanzierung missbraucht zu werden (s auch die Betonung der spezifischen Sachverhalte in Anhang 3 Kapitel E SPV). VT-Dienstleister haben, um dieses **Risiko zu identifizieren und entsprechend zu beherrschen**, unternehmensintern einen **risikobasierten Ansatz umzusetzen**: Sie müssen ihre **Risiken**, denen sie im Bereich der Geldwäscherei und Terrorismusfinanzierung ausgesetzt sind, selbständig **ermitteln**, bewerten und basierend auf den festgestellten Risiken entsprechende **Massnahmen ergreifen**, um den **Risiken** angemessen zu begegnen und diese auf ein vertretbares Mass **zu begrenzen** (Art 9–9b SPG).

Wie dieser risikobasierte Ansatz entwickelt und unternehmensintern implementiert wird, gibt das Gesetz nur abstrakt vor. Vieles hängt vom massgeblichen Geschäftsrisiko des Dienstleisters ab. Massnahmen zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung müssen nach der ratio legis jeweils mit den identifizierten Risiken im Einklang stehen. Die zur Verfügung stehenden Ressourcen sind zielgerichtet einzusetzen. Folglich ist dem Bereich mit den grössten Risiken auch die »grösste Aufmerksamkeit« zu widmen. Der Aufwand, der im Bereich der Erfüllung der Sorgfaltspflichten betrieben wird, hat demnach im Verhältnis zum potenziellen Risiko zu stehen. Die konkrete Ausgestaltung der Risikomatrix hat sich daher an der Art der vom VT-Dienstleister erbrachten Geschäfte bzw VT-Funktionen und den von ihm angebotenen Produkten und Dienstleistungen, an seinem Geschäfts- bzw Kundenstruktur (zB Nutzer des VT-Systems) sowie dem damit verbundenen Risikopotential zu orientieren.

A. Risikobewertung (Art 9a SPG)

VT-Dienstleister haben die für sie bestehenden Risiken in Bezug auf Geldwäscherei und Terrorismusfinanzie-

rung **individuell** zu ermitteln und **bewerten**. Die **Risikobewertung** ist durch jeden Sorgfaltspflichtigen für jede Geschäftskonstellation bzw Kundengruppe individuell vorzunehmen. Eine generelle Risikobewertung für eine gesamte Branche oder Berufsgruppe ist alleine nicht ausreichend.

Der Risikobewertung liegt jeweils eine **individuelle Risikoanalyse** zugrunde. Basierend auf dieser Risikoanalyse hat sodann die Zuordnung der Geschäftsbeziehungen und Transaktionen zum ausgewiesenen Risiko zu erfolgen. Zudem müssen geeignete interne Massnahmen festgelegt werden, um den identifizierten Risiken angemessen zu begegnen und zu überwachen.

Im Rahmen der individuellen Risikoanalyse haben Dienstleister die jeweils **angebotenen Produkte und Dienstleistungen** – unter spezifischem Einbezug der Verwendung neuer Technologien im Sinne des Art 9 Abs 2 SPG –, sowie die **individuelle Kundenstruktur** des Dienstleisters zu analysieren.

Im Rahmen der Risikoanalyse sind die Anhänge 1 und 2 des SPG zu berücksichtigen. Des Weiteren sind die massgeblichen Risikofaktoren aus den entsprechenden Leitlinien der Europäischen Aufsichtsbehörden zu den Risikofaktoren (JC GL 2017/37) zu verwenden. Daneben sind auch die im Rahmen der nationalen Risikoanalyse ausgewiesenen, relevanten Branchen-/und Produktrisiken zu berücksichtigen.

Nach erfolgter Risikoanalyse müssen sodann die **einzelnen Geschäftsbeziehungen** und Transaktionen entsprechend den **ausgewiesenen Risiken zugeordnet** werden, damit für die zuständigen Personen (zB Kundenbetreuer, Compliance, Prüfer etc) klar ist, welche Massnahmen im Einzelfall zu ergreifen sind. Basierend auf der Risikoanalyse müssen zudem geeignete **interne Kontroll- und Überwachungsmassnahmen** zur Minderung der genannten Risiken definiert werden. Diese Massnahmen – sowohl vereinfachte als auch verstärkte – beziehen sich einerseits auf den Umfang hinsichtlich der Erfüllung der Sorgfaltspflichten (zB Umfang des Geschäftsprofils, Umfang und Häufigkeit der Aktualisierung der Dokumentation, Höhe der Schwellenwerte bei der Überwachung etc) sowie andererseits auf die konkrete Ausgestaltung der internen Organisation (zB Umfang der internen Weisung, Benennung unterschiedlicher Personen für die internen Funktionen, etc).

Die konkrete Ausgestaltung und vor allem der Umfang und Detaillierungsgrad der Risikobewertung muss in einem angemessenen Verhältnis zur Art und Grösse des VT-Dienstleisters stehen. Konkret bedeutet das, dass die Risikobewertung des Dienstleisters, der beispielsweise sehr wenige Beschäftigte und nur **wenige Kunden** hat bzw **wenige Dienstleistungen** anbietet, prinzipiell auf ein **Minimum** reduziert werden kann.

Nochmals sei darauf hingewiesen, dass **registrierungspflichtige VT-Dienstleister** nach Art 3 Abs 1 Bst r SPG im Zuge der Risikobewertung unter Berücksichtigung des Stands der Technik **informatikgestützte Systeme einsetzen müssen, um risikobasiert die Historie der entsprechenden virtuellen Währungen bzw Token im entsprechenden VT-System (Art 2 Abs 1 Bst b TVTG) zu überprüfen.**

B. Risikoanalyse

Bei der **Erstellung der Risikobewertung** hat die Identifizierung potenzieller Risiken bei den jeweiligen Geschäftsbeziehungen zu erfolgen. Dabei hat der Dienstleister zu ermitteln, welche Risikofaktoren aufgrund der Geschäftstätigkeit bzw der Geschäftspolitik und Kundenstruktur für das Unternehmen von Relevanz sind. Es sind dabei jeweils sowohl risikoerhöhende als auch risikomindernde Faktoren zu berücksichtigen.

Bei den gesetzlich definierten Fällen mit erhöhten Risiken (Art 11 Abs 4–6 SPG) sind automatisch verstärkte Sorgfaltspflichten anzuwenden. Dabei ist unerheblich, ob der Dienstleister im Rahmen der individuellen Risikobewertung der betreffenden Geschäftsbeziehung allenfalls Faktoren und mögliche Anzeichen für ein potenziell geringeres Risiko identifiziert hat.

Neben den gesetzlich definierten Fällen erhöhter Risiken haben die VT-Dienstleister bei der Erstellung der Risikobewertung insbesondere die in den Anhängen 1 und 2 des SPG genannten Faktoren und mögliche Anzeichen für potenziell höhere bzw geringere Risiken und die Massnahmen bei Anwendung vereinfachter bzw verstärkter Sorgfaltspflichten sowie ergänzend die ESA-Leitlinien über Risikofaktoren zu berücksichtigen. Ebenso sind die Ergebnisse der nationalen Risikoanalyse zu beachten.

Sowohl die Anhänge des SPG als auch die in den ESA Leitlinien Risikofaktoren enthaltenen Faktoren sind nicht abschliessend. Zudem sind nicht alle Faktoren für sämtliche Branchen relevant. Die FMA erwartet daher für eine angemessene Umsetzung der Risikobewertung, dass jeweils die allgemeinen sowie die für die Branche relevanten Faktoren (zB »Token-Economy«) in der Risikobewertung entsprechend Berücksichtigung finden. Eine weitergehende Berücksichtigung zusätzlicher, über die ESA- und FMA-Vorgaben hinausgehende Faktoren ist daher nicht zwingend notwendig.

Bei der Risikoanalyse ist neben einer **Gesamtbeurteilung der Risikofaktoren** auch eine **angemessene Risikogewichtung** vorzunehmen. Ein einzelner Risikofaktor für sich allein erfordert in der Regel nicht die Zuordnung zu einer höheren oder niedrigeren Risikokategorie, relevant ist jeweils die Gesamtbetrachtung.

Die relevanten Risikofaktoren gliedern sich grundsätzlich in folgende vier Hauptkategorien, die im Rah-

men der Erstellung der Risikobewertung zu berücksichtigen sind:

- Kundenspezifische Faktoren (VT-Nutzerkategorisierung, anderer [sorgfaltspflichtiger] VT-Dienstleister);
- Produktbezogene Faktoren (zB Token-Typ);
- Vertriebsbezogene Faktoren (zB Art des VT-Systems und der Transaktionsmechanismen) und
- geografische Faktoren (Lage/Sitz der Server oder der dezentralen Hauptbücher).

Risikomindernde Faktoren für die Risikokategorisierung sind ua:

- Wohnsitz aller wirtschaftlich berechtigter Personen sowie allfälliger Ausschüttungsempfänger nach Art 7a SPG oder Begünstigter nach Art 7b SPG in einem EU-/EWR-Mitgliedsstaat oder in einem Drittstaat mit einem geringen geografischen Risiko;
- Sitz der Verwahrstelle eines Fonds in einem EU-/EWR- bzw gleichwertigen Drittstaat;
- Keine Involvierung von Rechtsträgern, die der privaten Vermögensverwaltung dienen;
- Häufiger Kontakt mit dem effektiven Vermögenseinbringer bzw der wirtschaftlich berechtigten Person;
- Keine Involvierung sensibler Branchen;
- Geringe Vermögenswerte;
- Geringes jährliches Transaktionsvolumen;
- Umfangreiche Informationen zum Zweck, Hintergrund und zur wirtschaftlichen Berechtigung der Geschäftsbeziehung;
- Verwendung spezifischer Produkte bzw Dienstleistungen wie zB Rentensysteme;
- Niederlassung bzw Repräsentanz in den Wohnsitzstaaten der wirtschaftlich berechtigten Personen bzw Mitarbeiter aus den betreffenden Regionen, welche die erforderlichen Sprachkenntnisse sowie das notwendige politische, soziokulturelle und regulatorische Hintergrundwissen zu den Herkunftsländern der wirtschaftlich berechtigten Personen mitbringen.

Risikoerhöhende Faktoren für die Risikokategorisierung sind ua:

- Wohnsitz einer wirtschaftlich berechtigten Person, eines Ausschüttungsempfängers nach Art 7a SPG oder eines Begünstigten nach Art 7b SPG in einem Drittstaat mit einem erhöhten geographischen Risiko;
- Involvierung von Rechtsträgern, die der privaten Vermögensverwaltung dienen; seltener Kontakt mit dem effektiven Vermögenseinbringer bzw der wirtschaftlich berechtigten Personen;
- Involvierung sensibler Branchen wie zB der Glücksspielsektor;

- Hohe Vermögenswerte;
- Hohes jährliches Transaktionsvolumen;
- Bargeldintensive Geschäftsbeziehung;
- Beschränkte Informationen zum Zweck, Hintergrund und zur wirtschaftlichen Berechtigung der Geschäftsbeziehung;
- Verwendung spezifischer Produkte bzw Dienstleistungen.

In diesem Zusammenhang ist zu beachten, dass Anhang 1 Abschnitt A Bst c SPG geografische Faktoren und mögliche **geografische Anzeichen** für ein potenziell geringeres Risiko anführt:

- EWR-Mitgliedstaaten;
- Drittstaaten, in denen Korruption und andere kriminelle Tätigkeiten laut glaubwürdigen Quellen schwach ausgeprägt sind;
- Drittstaaten, deren Anforderungen an die Bekämpfung von Geldwäsche und Terrorismusfinanzierung laut glaubwürdigen Quellen (zB gegenseitige Evaluierungen, detaillierte Bewertungsberichte oder veröffentlichte Follow-up-Berichte) den FATF-Empfehlungen 2012 entsprechen und die diese Anforderungen wirksam umsetzen. Auch hier ist insbesondere wieder auf den Wohnsitz der wirtschaftlich berechtigten Personen, der Ausschüttungsempfänger nach Art 7a SPG bzw der Begünstigten nach Art 7b SPG abzustellen (vgl Anhang 1 Abschnitt A Bst a Ziff 3 SPG). Bei Drittstaaten, die die oben genannten Kriterien erfüllen, gleichzeitig jedoch ein erhöhtes Korruptionsrisiko oder Terrorismusfinanzierungsrisiko aufweisen oder von Sanktionen, Embargos oder ähnlichen Massnahmen betroffen sind, ist eine Gesamtbetrachtung der geografischen Risiken vorzunehmen (FMA-Richtlinie 2013/1).

C. Zuordnung der Geschäftsbeziehungen und Transaktionen zu den Risikokategorien

Damit die Risikobewertung in der Praxis effektiv greift, müssen VT-Dienstleister die einzelnen **Geschäftsbeziehungen** und Transaktionen **den identifizierten Risiken zuordnen**. Diese Zuordnung hat durch ein Risikokategorisierungssystem zu erfolgen. Nur durch eine solche Kategorisierung und Zuordnung bzw Kennzeichnung der Geschäftsbeziehungen können die zuständigen Mitarbeiter die in der Risikobewertung vorgesehenen Massnahmen zur Anwendung bringen.

Die **Risikokategorisierung** soll eine sinnvolle Umsetzung und Anwendung des risikobasierten Ansatzes gewährleisten und muss folglich eine Abstufung enthalten, um nicht ins Leere zu laufen. Eine einzelne Risikokategorie für sämtliche Geschäftsbeziehungen macht daher keinen Sinn und läuft dem Grundgedanken des

risikobasierten Ansatzes zuwider. Zudem definiert bereits der Gesetzgeber die Kategorie erhöhter Risiken, welche sich in der Praxis hinsichtlich der Massnahmen von denen bei »normalen Risiken« abzugrenzen haben. Dadurch wird klargestellt, dass die verstärkten Massnahmen zusätzlich zu den regulären Massnahmen anzuwenden sind.

Die Festlegung der **Anzahl an Kategorien** bleibt den Dienstleistern überlassen. Je mehr Risikokategorien festgelegt werden, desto besser können die einzelnen Massnahmen auf die jeweiligen Risiken zugeschnitten werden. Eine Kategorie mit einem »Nullrisiko« kann es nicht geben. Die FMA empfiehlt in diesem Zusammenhang grundsätzlich eine Wahl von **vier Kategorien**:

- Geringe Risiken (vereinfachte Sorgfaltspflichten, Art 10 SPG);
- Vereinfachte Sorgfaltspflichten (Art 10 iVm Anhang 1 SPG, Art 18 Abs 2 und Art 22b SPV) dürfen ausschliesslich dann zur Anwendung gebracht werden, wenn die Sorgfaltspflichtigen ein geringes Risiko in Bezug auf Geldwäsche, organisierte Kriminalität und Terrorismusfinanzierung in ihrer Risikobewertung festgestellt und sich vergewissert haben, dass die betroffene Geschäftsbeziehung bzw Transaktion tatsächlich mit einem geringen Risiko verbunden ist. Die Anwendung der vereinfachten Sorgfaltspflichten ist gemäss Art 27 Abs 1 Bst c^{bis} SPV in den Sorgfaltspflichtakten bzw in anderen geeigneten internen Dokumenten (Risikomatrix oder Mandatsliste) zu dokumentieren.
- Normale Risiken (reguläre Sorgfaltspflichten);
- Erhöhte Risiken (verstärkte Sorgfaltspflichten nach Art 11 Abs 1 SPG, individuelle Risiken);
- In Fällen gesetzlich vorgesehener verstärkter Sorgfaltspflichten (Art 11 Abs 4 bis 6 SPG) besteht kein Ermessensspielraum hinsichtlich der Anwendung von verstärkten Sorgfaltspflichten. Lediglich hinsichtlich Art und Umfang der anzuwendenden Massnahmen besteht ein gewisser Anwendungsspielraum, vorausgesetzt, einzelne Massnahmen sind nicht bereits zwingend vom Gesetz vorgegeben (zB Art 11 Abs 4 und 4a SPG bei PEP).
- Hohe Risiken (verstärkte Sorgfaltspflichten nach Art 11 Abs 4 bis 6 SPG, automatische Fälle verstärkter Sorgfaltspflichten).

Es obliegt den VT-Dienstleistern, abhängig von Art und Umfang ihrer Geschäftstätigkeit die von der FMA vorgeschlagene 4-stufige Kategorisierung weiter auszubauen bzw einzugrenzen (zB erhöhte und hohe Risiken können in einer Kategorie zusammengefasst werden).

Die Kategorisierung muss nachvollziehbar dokumentiert und in der Praxis umgesetzt werden. Die Zuordnung einzelner Transaktionen bezieht sich auf die

jenigen Branchen, die typischerweise nur gelegentliche Transaktionen ausführen sowie auf diejenigen, für die die Aufnahme einer Geschäftsbeziehung der Ausnahmefall darstellt (zB Agenten von Banken).

D. Festlegung wirksamer interner Kontroll- und Überwachungsmassnahmen zur Minderung der Risiken

Basierend auf ihrer Risikobewertung haben VT-Dienstleister sodann entsprechende **interne Kontroll- und Überwachungsmassnahmen** festzulegen, um die identifizierten Risiken zu mindern. Das bedeutet, dass VT-Dienstleister ihre Sorgfaltspflichten (Art 5 Abs 1 SPG) risikoangemessen ausgestalten müssen. Die daran anknüpfende, zwingend zu führende Dokumentation (Art 20 SPG) muss daher das jeweils individuell ermittelte Risiko der Geschäftsbeziehung korrekt widerspiegeln und auch Aussagen zu den getroffenen Überwachungsmassnahmen enthalten. Daran knüpft auch die Ausgestaltung der internen Organisation, zumal diese dem individuellen Risiko des Dienstleisters Rechnung tragen muss (Art 21 Abs 2 SPG).

E. Dokumentation und Aktualität der Risikobewertung

VT-Dienstleister haben ihre **Risikobewertung zu dokumentieren** und stets aktuell halten. Zu beachten ist dabei, dass auch die jeweilige Zuordnung der Geschäftsbeziehungen und Transaktionen der aktuellen Risikosituation Rechnung tragen muss. Die Prüfung der Aktualität der Risikobewertung sowie die Festlegung von entsprechenden Massnahmen sind daher in periodischen Abständen auf ihre Angemessenheit hin zu überprüfen. Eine Aktualisierung hat mindestens alle drei Jahre zu erfolgen und darüber hinaus auch bei relevanten Änderungen der Kundenstruktur bzw der Geschäftstätigkeit des VT-Dienstleisters sowie bei neuen, für die Risikobewertung bedeutenden, relevanten branchenspezifischen Ergebnissen aus der nationalen Risikoanalyse.

Die **Aktualisierung** basierend auf Ergebnissen der nationalen Risikoanalyse hat jeweils spätestens ein Jahr nach deren Publikation zu erfolgen. VT-Dienstleister haben daher basierend auf ihren praktischen Erfahrungen zu beurteilen, ob sowohl die Risikoanalyse als auch die festgelegten Massnahmen und die Zuordnung der Geschäftsbeziehungen noch aktuell und angemessen sind. Dies ist entsprechend zu dokumentieren (Art 20 SPG).

Die Form der Dokumentation (physisch oder elektronisch) ist grundsätzlich dem VT-Dienstleister überlassen. Die Risikobewertung kann daher als Bestandteil der internen Weisungen ausgestaltet oder aber auch in

einem anderen geeigneten internen Dokument verarbeitet werden. Entscheidend ist, dass die Dokumentation so ausgestaltet wird, dass sie fachkundigen Dritten ein zuverlässiges Urteil über die individuelle Risikosituation des VT-Dienstleisters sowie die damit einhergehenden Massnahmen ermöglicht. Die Risikobewertung dient nämlich der individuellen organisatorischen Ausgestaltung des Dienstleisters und daher auch als Basis für Kontrollen. Sie ist daher den Prüfern anlässlich von Kontrollen zur Verfügung zu stellen.

F. Auswirkungen auf Sorgfaltspflichten des VT-Dienstleisters (Art 5 ff SPG)

Das jeweilige Risikoprofil des Dienstleisters hat ggfalls erhebliche **Auswirkungen auf seine geschäftliche** und wirtschaftliche Situation und Konsequenzen für Art und Ausmass der zu prästierenden Sorgfaltspflichten.

Die Häufigkeit der **Aktualisierung der Geschäftsprofile** ist vom jeweils ermittelten Risiko einer Geschäftsbeziehung abhängig. In jedem Fall müssen jegliche für das Geschäftsprofil bzw für die Überwachung der Geschäftsbeziehung relevanten Änderungen erfasst werden. In diesem Zusammenhang besteht eine aktive Prüf- und Aktualisierungspflicht der VT-Dienstleister hinsichtlich des gesamten Geschäftsbeziehungsbestands. Sie müssen folglich regelmässig prüfen, ob sämtliche im Rahmen des Geschäftsprofils gemäss Art 20 SPV zu erhebenden Informationen und Daten noch den tatsächlichen Gegebenheiten entsprechen.

Daher muss in individuell definierten, risikoangemessenen Abständen das einzelne Geschäftsprofil auf dessen Aktualität hin überprüft und bei Bedarf angepasst werden. Die Häufigkeit der Aktualisierung ist in den internen Weisungen bzw der individuellen Risikobewertung zu regeln (Art 31 Abs 2 Bst c^{bis} SPV).

In Fällen erhöhter oder hoher Risiken hat die **aktive Überprüfung** des Geschäftsprofils mindestens alle ein bis zwei Jahre stattzufinden. Im Fall normaler Risiken mindestens alle drei bis fünf Jahre. Im Fall geringer Risiken hat die Aktualisierung des Profils anlassbezogen (bspw anlässlich der Generierung eines »Alerts« des Überwachungssystems) zu erfolgen. Die Vorgaben bezüglich der Aktualisierungsintervalle gelten vorbehaltlich bekannter Änderungen vom Geschäftsprofil. Bekannte Informationen, die vom bestehenden Geschäftsprofil abweichen, sind daher jeweils unverzüglich im Geschäftsprofil zu berücksichtigen.

In der praktischen Umsetzung führt dies zu einer **aktiven Prüfpflicht** des VT-Dienstleisters. Dieser wird der Dienstleister etwa dadurch gerecht, dass er im Rahmen eines Kundengesprächs gezielt Fragen stellt, ob die Angaben im Geschäftsprofil (einschliesslich der wirtschaftlichen Berechtigung) noch den aktuellen Gegebenheiten

entsprechen. In der Regel ist der VT-Dienstleister aufgrund der bisherigen Kenntnis über den Kunden und des oftmals engen und regelmässigen Kundenkontakts bereits in der Lage, zeitnah Änderungen festzustellen und zu dokumentieren. Die **Aktualisierung** ist jeweils im Sinne von Art 20 Abs 3 SPV zu **dokumentieren** bzw intern zu vermerken.

Wenn sich im Rahmen der Überprüfung der Aktualität **keine Änderungen** ergeben, ist dieses Ergebnis zumindest in Form eines kurzen Vermerks bzw der Kenntlichmachung der Überprüfung zu dokumentieren. Eine explizite Formvorgabe existiert diesbezüglich nicht. Als ausreichend erachtet wird beispielsweise auch eine kurze Aktennotiz aus dem Kundengespräch oder auch ein tagesaktueller Ausdruck des Profils, solange diese die relevanten Informationen enthält.

Dem entsprechend sind auch **Geschäftsbeziehungen jeweils unterschiedlich engmaschig zu überwachen** (Art 9 SPG iVm Art 22 SPV). VT-Dienstleister müssen eine laufende, **risikoadäquate Überwachung aller Geschäftsbeziehungen** gewährleisten. Der Verlauf der Geschäftsbeziehung und die Abwicklung von Transaktionen müssen mit den Kenntnissen des Dienstleisters über den Kunden (VT-Nutzer) und dessen Geschäftsbeziehung und folglich mit dem Geschäftsprofil übereinstimmen. Wie auch die Anwendung der übrigen Sorgfaltspflichten hat die Überwachung entsprechend der Risikokategorisierung zu erfolgen. Das bedeutet, im Fall eines hohen oder erhöhten Risikos hat die laufende Überwachung engmaschiger und detaillierter zu erfolgen als in Fällen mit normalem oder gar geringem Risiko. Die Überwachung ist jedoch stets kontinuierlich und in regelmässigen Abständen vorzunehmen.

VT-Dienstleister haben stets auf Änderungen des Verhaltens bzw Abweichungen von typischen Verhaltensmustern des Kunden zu achten und aktiv nach Veränderungen im Zusammenhang mit den Angaben im Geschäftsprofil zu fragen.

IX. Sanktionen

Verletzungen der Sorgfaltspflichten durch VT-Dienstleister sind mit Verwaltungsgeldbussen von bis zu CHF 200.000 (in leichten Fällen), bei schwerwiegenden Rechtsverstössen mit bis CHF 5 Millionen bzw 10 % des vorjährigen Gesamtnettoumsatzes bedroht; die Sanktionen sind von der FMA zu verhängen. Neben dem Sorgfaltspflichtigen selbst können auch die verantwortlichen Mitglieder des Leitungsorgans strafrechtlich verfolgt werden (Art 30 Abs 1, 3 und 7 SPG).

X. Literatur

- ▶ *Damjanovic/Pfurtscheller/N. Raschauer*, Liechtensteins »Blockchain-Regulierung« – Ein- und Ausblicke, ZEuP 2021, 397
- ▶ *Fuchs*, Grundrechte in N. Raschauer/Wessely (Hrsg), VStG² (2016)
- ▶ *Lins/N. Raschauer*, Aufsicht über Gemeinden in G. Baumgartner (Hrsg), Recht der kommunalen Wirtschaftstätigkeit (2019) Rz 5.1 ff
- ▶ *Herzog*, Geldwäschegesetz³ (2018)
- ▶ *Müller/N. Raschauer*, Wirtschaftsaufsichts- und Regulierungsrecht in B. Raschauer/Ennöckl/N. Raschauer, Wirtschaftsrecht⁴ (2021) Rz 501 ff
- ▶ *Pfurtscheller/N. Raschauer/Stern*, Von regulatorischen Sandplätzen und Innovationsknotenpunkten – rechtsvergleichende Bemerkungen zur Förderung von Fintechs in der DACH-Region, ZFR 2021, 4
- ▶ *B. Raschauer/Storr*, Allgemeiner Teil in B. Raschauer/Ennöckl/N. Raschauer (Hrsg), Wirtschaftsrecht⁴ (2021)
- ▶ *N. Raschauer*, Aktuelle Strukturprobleme des europäischen und österreichischen Bankenaufsichtsrechts (2010)
- ▶ *N. Raschauer/Silbernagl*, Grundsatzfragen des liechtensteinischen »Blockchain-Gesetzes« – TVTG, ZFR 2020, 11
- ▶ *N. Raschauer/Stern*, Delegation und Auslagerungen von Sorgfaltspflichten – zugleich Anmerkungen zur Reichweite der Art 14 SPG und Art 24 ff SPV, LJZ 2020, 156
- ▶ *Roth*, Das Verhältnis zwischen verwaltungsrechtlichen Mitwirkungspflichten und dem Grundsatz nemo tenetur se ipsum accusare, ZStrR 2011, 296
- ▶ *Sild*, Blockchain Regulation made in Liechtenstein. Das Fürstentum als Vorreiter? SPWR 2020, 45

Korrespondenz:

Prof. Dr. Nicolas Raschauer
Bereich Wirtschaftsrecht
HSSH Schaffhausen, Schweiz,

Mail: nicolas.raschauer@hochschule-schaffhausen.ch.

PD Dr. Thomas Stern MBA,
stellvertretender Leiter der Abteilung
Aufsicht, Bereich Banken,
Finanzmarktaufsicht Liechtenstein,
Mail: tomek.stern@gmx.at.