Achtung: Diese Version der FMA-Wegleitung 2021/18 ist nicht mehr in Kraft. Diese Version war gültig vom 17. Mai 2022 bis zum 24. Januar 2023.

FMA
Finanzmarktaufsicht
Liechtenstein

Wegleitung 2021/18 Pflichten bei der Durchführung von VT-Transfers

Referenz:	FMA-WL 2021/18
Adressaten:	Sorgfaltspflichtige nach Art. 3 Abs. 1 Bst. r und t SPG
Betrifft:	Gesetz vom 11. Dezember 2008 über berufliche Sorgfaltspflichten zur Bekämpfung von Geldwäscherei, organisierter Kriminalität und Terrorismusfinanzierung (Sorgfaltspflichtgesetz; SPG) und die dazugehörige Verordnung (Sorgfaltspflichtverordnung, SPV)
Publikationsort:	Website FMA
Publikationsdatum:	18. August 2021
Letzte Änderung:	17. Mai 2022

Inhalt

Landstrasse 109 • Postfach 279 • 9490 Vaduz • Liechtenstein
Telefon +423 236 73 73 • Telefax +423 236 73 74 • www.fma-li.li • info@fma-li.li

1. Hintergrund

Mit Änderung des SPG vom 1. April 2021 wurde in Art. 12a SPG die Grundlage für den Informationsaustausch betreffend die Daten zu den Begünstigten und Auftraggebern einer Transaktion auf einem VT-System geschaffen. Mit Änderung der SPV vom 1. Juni 2021 wurden diese Regelungen in Art. 4 und 23b ff SPV konkretisiert. Diese Bestimmungen sollen nun in der folgenden Wegleitung erläutert und das Nähere dazu geregelt werden.

Die Empfehlung Nr. 15 der FATF-Empfehlungen sieht vor, dass bei Transfers von Token- oder virtuellen Währungen, ähnlich den Regelungen zur Geldtransferverordnung, ein Informationsaustausch hinsichtlich der Daten des Begünstigten und des Auftraggebers zwischen VT-Dienstleistern durchgeführt wird. Die hier vorliegende Erläuterung orientiert sich grundlegend an der Geldtransferverordnung sowie den Vorgaben der FATF-Empfehlung Nr. 16.

2. Anwendungsbereich

Gemäss Art. 23b SPV ist ein Informationsaustausch bei sämtlichen Transfers von Token- oder virtuellen Währungen (Token), welche gegenwärtig den Betrag von einem Franken übersteigen, notwendig. Die Regelung findet grundsätzlich Anwendung auf sämtliche Sorgfaltspflichtige gemäss Art. 3 Abs. 1 Bst. r und t SPG (VT-Dienstleister)[1].

Entscheidend für die Verpflichtung zum Informationsaustausch ist, dass der Token tatsächlich transferiert wird. Dies bedeutet, dass eine Übertragung in irgendeiner Form auf dem VT-System stattfindet, in welche der VT-Dienstleister eingebunden ist. Schlussendlich bedeutet dies, dass ein VT-Dienstleister, welcher eine Übertragung eines Token auf dem VT-System anstösst, durchführt, ausführt oder in Auftrag gibt[2], verpflichtet ist, einen Informationsaustausch durchzuführen, sofern auf der gegenüberliegenden Seite ebenso ein VT-Dienstleister eingebunden ist und der zu transferierende Betrag einen Franken übersteigt.

Sofern die Gegenpartei (auftraggebender oder begünstigender VT-Dienstleister, mit welchem ein VT-Transfer abgeschlossen wird) ein ausländischer Dienstleister ist, der bei Sitz im Inland ein nach dem Liechtensteinischen TVTG registrierungspflichtiger VT-Dienstleister wäre, besteht ebenso eine Verpflichtung zur Durchführung des Informationsaustausches. Dabei ist es möglich, dass der Dienstleister im Ausland ein registrierter Zahlungsdienstleister oder eine Bank ist. Ebenso ist ein Informationsaustausch durchzuführen, wenn der ausländische Dienstleister auf Grund seiner Tätigkeiten im Ausland der Anwendung der «Travel-Rule» unterliegt.

2.1. Ausnahmen

Token-Emittenten sind dann von dieser Verpflichtung ausgenommen, wenn der Transfer im Rahmen der Erstemission durchgeführt wird. Sofern darüber hinaus allerdings weitere Transfers durchgeführt werden (Sekundärmarkt), fallen auch Token-Emittenten in den Anwendungsbereich der Travel-Rule-Bestimmungen.

Wenn VT-Transfers auf einer White-Label-Plattform durchgeführt werden, sind diese VT-Transfers ebenso vom Anwendungsbereich der «Travel Rule» ausgenommen, da grundsätzlich ein zentraler Betreiber der White-Label-Plattform bereits vorab sämtliche Daten und Informationen der Nutzer im Rahmen des KYC einzuholen und zu überprüfen hat.

[1] In einem UTXO-System gilt als Transfer unabhängig von der Anzahl der Transaktionen der Übertrag von einer VT-Identifikator zu einer anderen VT-Identifikator, wobei Transaktionsgebühren und «change outputs» unbeachtet bleiben können.

[2] Im Falle eines VT-Dienstleisters, welcher einen Transfer bei einem Sub-Custodian in Auftrag gibt, ist der VT-Dienstleister zum Informationsaustausch verpflichtet und nicht der Sub-Custodian. Eine Delegation an den Sub-Custodian ist jedoch zulässig.

VT-Agenten sind insoweit von dieser Verpflichtung ausgenommen, soweit die Verpflichtungen vom ausländischen VT-Dienstleister, für welchen sie die Dienstleistungen vertreiben oder ausführen, übernommen werden.

Ausgenommen sind auch Eigentransfers zwischen zwei VT-Dienstleistern. Sofern allerdings nur aus Sicht eines VT-Dienstleisters ein Eigentransfer vorliegend ist, sind die Bestimmungen gemäss Art. 23b ff SPV anzuwenden. Unter einem Eigentransfer wird ein Transfer im eigenen Namen und auf eigene Rechnung des VT-Dienstleisters verstanden.

Zwischengeschaltete Servicedienstleister (Routing, Clearance, Betrieb eines Lightning Nodes…) sind soweit von der Verpflichtung zur Weiterleitung der Informationen ausgenommen, als dies für den Informationsaustausch zwischen den VT-Dienstleistern nicht notwendig ist.

3. Feststellung der Gegenpartei

Um den Informationsaustausch durchzuführen, ist es notwendig festzustellen, ob es sich bei der Gegenpartei um einen begünstigenden VT-Dienstleister (allenfalls ein auftraggebender VT-Dienstleister) handelt, oder nicht. Diese Feststellung der Gegenpartei ist somit für jeden Transfer von Token mit einem Gegenwert von mehr als einem Franken relevant.

Der Gesetzgeber gibt vor, dass vor dem Abschluss eines VT-Transfers eine Feststellung der Gegenpartei zu erfolgen hat. Auf welche Art und Weise diese durchzuführen ist, lässt er offen. Der Abschluss des VT-Transfers liegt dann vor, wenn der Begünstigte bzw. der Auftraggeber über die transferierten Token frei verfügen kann. Sofern beispielsweise die transferierten Token im Account des Begünstigten gesperrt bleiben, liegt noch kein Abschluss des VT-Transfers vor.

Zur Feststellung der Gegenpartei können verschiedene Verfahren angewendet werden. Einerseits kann eine Feststellung über die Nutzung eines Standards erfolgen, welche beispielsweise eine Feststellung mittels Führen eines zentralen VASP-Registers oder durch Verifizierung der Gegenpartei mittels Smart-Contract durchführen. Andererseits kann vorläufig die Gegenpartei beispielsweise festgestellt werden, indem der VT-Identifikator anhand eines Blockchaintrackingtools mit einer hohen Wahrscheinlichkeit einer bestimmten Gegenpartei zugeordnet wird oder durch Mitteilung des Auftraggebers oder Begünstigten, dass es sich um eine bestimmte Gegenpartei handelt. Letzteres ist insbesondere dann relevant, wenn die entwickelten Standards noch nicht entsprechend umsetzbar oder anwendbar sind.

Als vertrauenswürdige zentrale VASP-Register werden jedenfalls diejenigen Register, welche von Aufsichtsbehörden oder sonstigen internationalen oder supranationalen Organisationen geführt werden. Grundsätzlich sind auch Register, welche von Dienstleistern im Zusammenhang mit Travel Rule Durchführungsanwendungen geführt werden und von diesen Dienstleistern auch eine Überprüfung der im Register eingetragenen Personen erfolgt, vertrauenswürdig.

Nach der Feststellung eines begünstigenden VT-Dienstleisters (oder allenfalls auftraggebenden VT-Dienstleisters) als Gegenpartei ist dieser auch zu verifizieren. Dabei ist Einblick in das Register der zuständigen Aufsichtsbehörde zu nehmen oder durch Abgleich anderer öffentlich verfügbaren und vertrauenswürdigen Register eine Verifikation dieser Gegenpartei durchzuführen. Allenfalls kann auch im Rahmen der Abstimmung über die Informationsübermittlung eine Verifikation durchgeführt werden. Bei Nutzung eines Standards erfolgt dies in der Regel automatisch.

Nach Durchführung der Verifikation ist mit dieser Gegenpartei der Weg der Informationsübermittlung abzustimmen.

4. Informationsaustausch

Der Informationsaustausch hat auf sichere Weise vor dem Abschluss des VT-Transfers zu erfolgen. Auf sichere Weise bedeutet, dass der Übermittlungsweg nach dem aktuellen Stand der Technik abzusichern ist.

Sofern ein Standard zur Übermittlung der Informationen genutzt wird[3], kann grundlegend davon ausgegangen werden, dass eine sichere Übermittlung vorliegt. Grundsätzlich kann ein Informationsaustausch auch ausserhalb der Nutzung eines Standards erfolgen.

4.1. Erhebung der Informationen durch den auftraggebenden VT-Dienstleister

Vor dem Informationsaustausch sind nachfolgende Informationen durch den auftraggebenden VT-Dienstleister zu erheben:

- der Name (Vor- und Nachname/Firmenname) des Begünstigten und des Auftraggebers;
- die Bezeichnung oder Nummer des VT-Kontos (bspw. der VT-Identifikator) des Auftraggebers und des Begünstigten; sowie
- die Adresse und das Land (Wohnsitz/Sitz), die Nummer eines gültigen amtlichen Ausweises, die Kundennummer oder das Geburtsdatum und der Geburtsort des Auftraggebers.

Der auftraggebende VT-Dienstleister hat Massnahmen und Strategien zu implementieren, welche gewährleisten, dass sämtliche Informationen hinsichtlich des Auftraggebers vor dem Informationsaustausch verifiziert, korrekt und übermittlungsfähig sind. In der Regel finden sich diese Informationen im Geschäftsprofil zum Kunden und werden bei Aufnahme der Geschäftsbeziehung erfasst und verifiziert.

Hinsichtlich Betreibern von physischen Wechselautomaten, welche gemäss Art. 5 Abs. 2 Bst. h SPG erst ab einem Schwellenwert von 1000 Franken sorgfaltspflichtig sind, gilt die Feststellungs- und Verifizierungspflicht im Rahmen des Informationsaustausches ebenso ab einem Schwellenwert von einem Franken. Dies bedeutet, dass eine eingeschränkte KYC-Pflicht bereits ab einem Schwellenwert von einem Franken beginnt.

Weiters hat der auftraggebende VT-Dienstleister Massnahmen und Strategien zu implementieren, die sicherstellen, dass die Informationen zum Begünstigten eingeholt wurden und diese zudem übermittlungsfähig und nicht unsinnig sind, wobei die Informationen zum Begünstigten nicht zu verifizieren sind.

Schlussendlich darf der VT-Transfer erst aus- oder durchgeführt bzw. vom auftraggebenden VT-Dienstleister angestossen werden, wenn sämtliche für die Durchführung des Informationsaustauschs relevanten Informationen vorliegen.

4.2. Sanktions-Screening durch den auftraggebenden VT-Dienstleister

Neben der Verifizierung der Auftraggeberdaten obliegt dem auftraggebenden VT-Dienstleister auch die Verpflichtung zum Sanktions-Screening. Dieses ist grundsätzlich sowohl für die Auftraggeber-Informationen als auch für die Begünstigten-Informationen durchzuführen. Neben dem VT-Konto ist auch ein Abgleich des Namens des Auftraggebers/Begünstigen durchzuführen.

4.3. Einholung der Informationen durch den begünstigenden VT-Dienstleister

Der begünstigende VT-Dienstleister hat die Informationen zum Begünstigten einzuholen und zu verifizieren. In aller Regel erfolgt dies bereits im Rahmen des Onboarding/KYC-Prozesses bei Geschäftsaufnahme mit dem Begünstigten.

4.4. Sanktions-Screening durch den begünstigenden VT-Dienstleister

Neben der Verifizierung der Daten des Begünstigten obliegt dem begünstigenden VT-Dienstleister auch die Verpflichtung zum Sanktions-Screening. Dies ist grundsätzlich sowohl für die Auftraggeber- als auch für die

[3] Beispielsweise das “Travel Rule Protocol (TRP)“ oder „OpenVASP“.

Begünstigten-Informationen durchzuführen. Neben dem VT-Konto ist auch ein Namensabgleich durchzuführen.

Das Sanktionsscreening hat vor dem Abschluss des VT-Transfers zu erfolgen.

4.5. Plausibilisierung der Informationen durch den begünstigenden VT-Dienstleister

Nach der Übermittlung der Informationen hat der begünstigende VT-Dienstleister die relevanten Informationen auf deren Vollständigkeit zu prüfen. Weiters hat die Plausibilisierung auch eine Analyse der Richtigkeit und Sinnhaftigkeit der Daten zu beinhalten. So ist beispielsweise zu prüfen, ob beim Namensfeld auch tatsächlich ein Name eingetragen wurde und nicht eine x-beliebige Zeichenfolge oder gar unsinnige Angaben wie „mein Kunde“. Beim „VT-Identifikator des Auftraggebers“ ist beispielsweise zu prüfen, ob es sich bei dieser auch tatsächlich um eine Adresse des jeweiligen VT-Systems handelt.

In weiterer Folge hat der begünstigende VT-Dienstleister die übermittelten Informationen zum Begünstigten auf deren Korrektheit zu überprüfen, indem ein Abgleich mit den selbst eingeholten und verifizierten Informationen zum Begünstigten erfolgt.

Die Überprüfung der übermittelten Informationen hat vor dem Abschluss des VT-Transfers zu erfolgen. Die Token dürfen dem Begünstigten erst dann zur freien Verfügung stehen, wenn sämtliche Informationen korrekt und vollständig vorliegen und der Sanktionscheck negativ war.

4.5.1. Unvollständige oder nicht übermittelte Informationen

Der begünstigende VT-Dienstleister hat wirksame Verfahren und Strategien zu implementieren um feststellen zu können, ob die Informationen nicht oder nur unvollständig übermittelt wurden. Solche wirksamen Verfahren zeichnen sich dadurch aus, dass einerseits eine unvollständige oder fehlende Übermittlung erkannt und andererseits der VT-Transfer nicht abgeschlossen werden kann. Sofern Informationen fehlen oder unvollständig sind, ist in einem ersten Schritt binnen dreier Werktage eine Korrektur/Verbesserung vom auftraggebenden VT-Dienstleister anzufordern. Sofern der auftraggebende VT-Dienstleister dieser Frist nicht nachkommt, ist der VT-Transfer zurückzuweisen oder retour zu transferieren. Sofern der VT-Transfer nicht zurückgewiesen werden kann, ist allenfalls ein Re-Transfer der Token durchzuführen.

4.5.2. Unsinnige und inkorrekte Angaben

Der begünstigende VT-Dienstleister hat wirksame Verfahren und Strategien zu implementieren um feststellen zu können, ob die Informationen inkorrekt oder unsinnig übermittelt wurden. Solche Verfahren werden dann als wirksam erachtet, wenn einerseits unsinnige oder inkorrekte Informationen erkannt werden können und andererseits, dass der VT-Transfer in solchen Fällen nicht abgeschlossen werden kann. Wenn beispielsweise ein VT-Identifikator aus 27-34 alphanummerischen Zeichen zu bestehen hat, in der Übermittlung jedoch nur 26 Zeichen dargestellt werden, so ist die Information inkorrekt. Sofern die Informationen unsinnig sind, ist in einem ersten Schritt der auftraggebende VT-Dienstleister dazu aufzufordern, die korrekten Informationen binnen dreier Werktage zu übermitteln. Sofern der auftraggebende VT-Dienstleister dieser Aufforderung nicht nachkommt, ist der VT-Transfer zurückzuweisen. Sofern die Informationen inkorrekt sind, hat eine einfache Abklärung im Sinne von Art. 9 Abs. 3 SPG zu erfolgen. Im Rahmen der einfachen Abklärung kann ein weiterer Informationsaustausch zum Sachverhalt mit dem auftraggebenden VT-Dienstleister erfolgen oder beispielsweise eine Wiederholung der Feststellung und Überprüfung der Identität des Vertragspartners und der wirtschaftlich berechtigten Person. Sofern die einfache Abklärung nicht zur vollständigen Aufklärung führt, ist eine Verdachtsmitteilung an die SFIU zu übermitteln und die Vermögenswerte sind vorübergehend einzufrieren.

4.5.3. Verspätet übermittelte Angaben

Der begünstigende VT-Dienstleister hat wirksame Verfahren und Strategien zu implementieren um feststellen zu können, ob die Informationen verspätet übermittelt werden. Sofern die Informationen verspätet übermittelt werden, kann der begünstigende VT-Dienstleister den auftraggebenden VT-Dienstleister auffordern, die Informationen unverzüglich zu übermitteln. Allenfalls kann der begünstigende VT-Dienstleister ohne weiteres den VT-Transfer ab- oder zurückweisen oder ein Re-Transfer durchführen.

5. Massnahmen im Hinblick auf wiederholt säumige VT-Dienstleister

Sorgfaltspflichtige haben iZm der Übermittlung der Informationen Strategien und Verfahren für die Fälle vorzusehen, in welchen der gegenüberliegende VT-Dienstleister wiederholt säumig ist, diese überhaupt nicht oder unvollständige, unsinnige oder unkorrekte Informationen übermittelt. Um feststellen zu können, ob ein VT-Dienstleister wiederholt säumig ist, müssen einerseits Verfahren implementiert werden, welche es erlauben, die einzelnen fehlerhaften Informationsübermittlungen einem VT-Dienstleister zuzuschreiben. Weiters muss festgelegt werden, anhand welcher Kriterien eine wiederholte Säumigkeit angenommen werden soll. Dies kann beispielsweise anhand eines bestimmten Prozentsatzes sämtlicher Transaktionen oder andererseits anhand eines absoluten Wertes bestimmt werden. Weiters ist auch relevant, ob der gegenüberliegende VT-Dienstleister im Rahmen von Abklärungen kooperativ ist oder nicht.

Sofern festgestellt wird, dass ein VT-Dienstleister wiederholt säumig ist, müssen weitere Massnahmen ergriffen werden. Je nach Schweregrad der Verfehlung können unterschiedliche Eskalationsstufen ergriffen werden. Diese können eine Durchführung oder Wiederholung der Due Diligence der Gegenpartei (siehe Ziff. 6), eine Verwarnung, eine vorübergehende oder gänzliche Untersagung weiterer VT-Transfers oder in Fällen, in welchen die Gegenpartei bereits einer «Travel-Rule-Anforderung» in ihrem Sitzstaat unterliegt, auch eine Meldung an die zuständige Aufsichtsbehörde im Inland (FMA) sein. Im Rahmen einer solchen Meldung sind sämtliche Unterlagen zu den VT-Transfers, den Verfehlungen und der Gegenpartei selbst zu übermitteln.

6. Überprüfung der Gegenpartei

Sofern mit einer Gegenpartei in einem Hochrisikoland (Geldwäsche oder Terrorismusfinanzierung) mehrmals ein VT-Transfer abgeschlossen wird, sind diese Gegenparteien einem eingehenden Monitoring zu unterziehen um das Risiko von VT-Transfers mit Geldwäschebezug oder Terrorismusfinanzierung zu reduzieren. Die Überprüfung der Gegenpartei erfolgt analog zu Korrespondenzbankbeziehungen[4] und sollte stets unter Einholung der Zustimmung der Leitungsebene erfolgen. Neben der Überprüfung, ob die Gegenpartei einer Aufsicht untersteht, sollte der Schwerpunkt der Überprüfung auf der Bewertung des «Risk Exposure» hinsichtlich des Bezugs zu Vortaten der Gegenpartei anhand eines Blockchaintrackingtools sowie eines adäquaten Know Your Customer-Prozesses gelegt werden. Dabei kann auch auf unabhängige, zuverlässige Quellen zurückgegriffen werden. Zudem sollte die Gegenpartei auch in regelmässigen risikobasierten Abständen einer Due Diligence Prüfung unterzogen werden, welche das «Risk Exposure» hinsichtlich dem Bezug zu Vortaten und eine Medienrecherche, die Qualität des Informationsaustausches sowie eine direkten Befragung – beispielsweise des Wolfsberg Questionnaires[5] – beinhaltet.

Der risikobasierte Ansatz zur Wiederholung der Due Diligence Prüfung orientiert sich insbesondere an der Qualität des Informationsaustausches und an den Feststellungen hinsichtlich Adverse Media.

Hohe geographische Risiken liegen insbesondere dann vor, wenn die Gegenpartei ihren Sitz in einem Tier 1-3-Land gemäss des Global Terrorism Indizes[6] oder einem Land gemäss Anhang 4 der SPV[7] oder einem Land mit strategischen Defiziten nach FATF gemäss Liste A[8] der FMA hat.

Sofern ein hohes oder erhöhtes Risiko von der Gegenpartei ausgeht, unterliegen VT-Transfers grundlegend verstärkten Sorgfaltspflichten. Dies schlägt sich einerseits in der verstärkten Überprüfung und Überwachung

[4] Vgl. hierzu Ziff. 6.6 der FMA-Wegleitung 2018/7, Kapitel II VT-Dienstleister.

[5] https://www.wolfsberg-principles.com/wolfsbergcb

[6] https://www.visionofhumanity.org/wp-content/uploads/2020/11/GTI-2020-web-1.pdf

[7] https://www.gesetze.li/konso/2009.98

[8] Jurisdiktionen unter erhöhter Beobachtung der FATF (Liste A – Erhöhte geografische Risiken gemäss Anhang 2 Abschnitt A Bst. c SPG).

der Gegenpartei und andererseits in der vertieften Abklärung des VT-Transfers nieder. Letzteres kann beispielsweise durch Übermittlung der KYC-Informationen durch die Gegenpartei erfolgen.

7. Massnahmen bei Transfers, welche nicht der «Travel Rule» unterliegen

Sofern ein VT-Transfer nicht der «Travel Rule» unterliegt, da es sich bei der Gegenpartei um keinen VT-Dienstleister oder kein ausländisches Äquivalent dazu handelt, sind auf diese Transaktion verstärkte Sorgfaltspflichten anzuwenden. Unabhängig von der sonstigen Einstufung der Geschäftsbeziehung sind Massnahmen zu ergreifen, die das durch die fehlende Verifizierung der Gegenpartei verbundene Risiko reduzieren. Die Sorgfaltspflichtigen haben deshalb angemessene Verfahren und Strategien zur Risikoreduzierung zu implementieren. Als Mittel zur Risikoreduzierung ist bei unhosted/private wallets jedenfalls ein «proof of ownership» durchzuführen. Weitere Mittel können bspw. die Einholung und Prüfung von Drittbelegen sein, anhand welcher der Zweck und das Volumen des Transfers plausibilisiert werden kann. Zudem sind solche Transaktionen jedenfalls mittels eines Blockchaintrackingtools zu analysieren.

Sofern VT-Transfers mehrmals von dem/an das gleiche unhosted/private wallet transferiert werden, muss nicht bei jedem Transfer ein «proof of ownership» durchgeführt werden. Es ist ausreichend, wenn dieser in risikobasierten Abständen (jährlich oder bei sonstigen Anzeichen, dass ein Eigentümerwechsel des wallets stattgefunden hat) wiederholt wird.

8. Dokumentation

Im Sorgfaltspflichtakt sind sämtliche Unterlagen den Transaktionen zugeordnet zu dokumentieren. Insbesondere sind auch sämtliche getroffenen Massnahmen zu dokumentieren. Neben den Transaktionsdaten, den Informationen zum Auftraggeber und Begünstigten, sind auch die Gegenpartei und der Sitz der Gegenpartei sowie sämtliche getroffenen Massnahmen und Abklärungen im Zusammenhang mit Ziff. 4, 5 und 7 dieser Wegleitung zu dokumentieren.

Im Hinblick auf das jährliche Meldewesen sind die Transaktionsdaten so abzulegen, dass das Transaktionsvolumen und der Sitz der Gegenpartei auswertbar sind.

Sofern des Öfteren mit einer Gegenpartei korrespondiert wird, sind die getroffenen Massnahmen zur Überprüfung der Gegenpartei zu dokumentieren. Diesbezüglich empfiehlt sich die Anlage eines «VASP-Registers».

9. Interne Weisung

Die Strategien und Verfahren sowie die zugehörigen Prozesse im Zusammenhang mit den Anforderungen der «Travel Rule» sind in die internen Weisungen des Sorgfaltspflichtigen einzupflegen.

10. «Sunrise-Problematik»

Im Zusammenhang mit der globalen Umsetzung der «Travel Rule» werden einerseits unterschiedliche Ansätze in der Regulierung verfolgt und andererseits gibt es gravierende Unterschiede im Fortschritt dieser Regulierung[9]. Aus europäischer Sicht ist mit einer vollständigen Implementierung auf Grundlage der Geldtransferverordnung zudem erst mit 2024 zu rechnen.[10] So haben manche Länder die «Travel Rule» bereits

[9] Vgl. hierzu auch 2nd 12-month review of revised FATF standards Virtual Assets and VASPs und auch Travel Rule Compliance Report (Notabene).

[10] Vgl. die Übergangsfrist hinsichtlich der Änderung der Geldtransferverordnugn (VO (EU) 847/2015): https://www.europarl.europa.eu/doceo/document/A-9-2022-0081_EN.html

vollständig in ihren gesetzlichen Vorgaben implementiert, manche Länder haben zusätzlich weitreichende Übergangsfristen vorgesehen und viele Länder haben bislang noch keine Regelungen in diesem Zusammenhang vorgegeben.

Unabhängig von der Standarddiskussion oder Problematik um die Feststellung der Gegenpartei erschweren die unterschiedlichen rechtlichen Vorgaben weltweit die aktive Implementierung der «Travel Rule»-Anforderungen bei den Sorgfaltspflichtigen. Beispielsweise können grosse ausländische VT-Dienstleister nicht zum Informationsaustausch verpflichtet sein, von diesen abhängige inländische VT-Dienstleister jedoch schon. Da die Umsetzung mit wesentlichem Aufwand verbunden ist, dürfte in solchen Fällen das Engagement des ausländischen VT-Dienstleisters zur Umsetzung des Informationsaustausches gering sein und schlussendlich wird es dem inländischen abhängigen VT-Dienstleister nur schwer möglich sein, die Anforderungen an den Informationsaustausch einzuhalten.

Technische Implementierung:

In erster Linie sollte die technische Implementierung für die Einholung der Informationen zum VT-Transfer (Auftraggeber und Begünstigtendaten) sowie die entsprechenden Screening-Massnahmen und Massnahmen im Zusammenhang mit Transfers von/zu unhosted/private wallets durchgeführt werden. Die Implementierungsmassnahmen sollten grundlegend bereits abgeschlossen sein.

Informationsaustausch mit Gegenparteien:

Diesbezüglich ist vom inländischen VT-Dienstleister risikobasiert vorzugehen wie folgt:

Nach erfolgter technischer Implementierung ist die Durchführung eines Informationsaustauschs mit der Gegenpartei anzustreben. Sofern dies von der Gegenpartei abgelehnt werden sollte, ist dies zu dokumentieren. In weiterer Folge ist eine entsprechende Risikobewertung vorzunehmen, wie in Ziff. 8 dieser Wegleitung beschrieben. Sofern die Gegenpartei ihren Sitz in Ländern hat, welche grundlegend ein hohes GW/TF-Risiko vorweisen, sind entsprechende Massnahmen zur Reduzierung des Transferrisikos zu treffen. Sofern die Gegenpartei aus dem EU/EWR-Raum oder einem gleichwertigen Drittstaat im Sinne des Anhang 1 der FMA-Wegleitung 2018/7 stammt, darf längstens ein VT-Transfer ohne Informationsaustausch bis zum 31. Dezember 2023 abgeschlossen werden. Für Gegenparteien aus sämtlichen anderen Jurisdiktionen darf längstens ein VT-Transfer ohne Informationsaustausch bis zum 31. Dezember 2022 abgeschlossen werden. Bei sämtlichen VT-Transfers, bei welchen dieser risikobasierte Ansatz angewendet wird, sind verstärkte Sorgfaltspflichten anzuwenden und entsprechende Massnahmen zur Reduzierung des Risikos anzuwenden. Unabhängig davon sind sämtliche Vorgaben (ausgenommen Informationsaustausch) einzuhalten. Die Strategien und Verfahren hinsichtlich des risikobasierten Ansatzes sind in der internen Weisung vorzuschreiben.

Diese risikobasierte Vorgehensweise ist bei Gegenparteien in Ländern, welche bereits eine vollumfängliche Implementierung der «Travel Rule» vorschreiben, nicht anzuwenden. Mit Gegenparteien aus solchen Ländern ist stets ein Informationsaustausch durchzuführen.

11. Datenschutz

Der Inhalt dieser Wegleitung lässt die Vorgaben der Datenschutzgesetzgebung unberührt. Die Sorgfaltspflichtigen haben daher in Umsetzung dieser Wegleitung stets die Vorgaben des Datenschutzes – insbesondere der Datenschutz-Grundverordnung (EU) 2016/679 zu befolgen.

12. Schlussbestimmungen

12.1. Inkrafttreten

Diese Wegleitung tritt mit 18. August 2021 in Kraft.

Die Änderungen vom 17. Mai 2022 treten am selben Tag in Kraft.

Stand: 17. Mail 2022

13. Änderungsverzeichnis

Mit 17. Mai 2022 wurden folgende Änderungen vorgenommen:

Ziff. 2.1 Klarstellung, dass VASP-2-VASP-Eigentransfers vom Anwendungsbereich ausgenommen sind.

Ziff. 4.1 Einholung der Adresse und des Landes des Auftraggebers.

Ziff. 6 Erweiterung um Länder mit strategischen Defiziten nach FATF, welche in der SPV nicht enthalten sind.

Ziff. 7 Erweiterung, dass ein «proof of ownership» jedenfalls durchzuführen ist – dieser allerdings bei Mehrfachtransfers risikobasiert erfolgen kann.

Ziff. 10 Verlängerung des risikobasierten Ansatzes (sunrise issue) und Klarstellung, dass das Augenmerk auf die technische Implementierung zur Einholung von Informationen und Durchführung entsprechender Massnahmen gelegt werden soll.