FMA

Finanzmarktaufsicht
Liechtenstein

Wegleitung 2019/7 zu den im Sinne von Art. 14 Abs. 1 SPV anwendbaren Sicherungsmassnahmen bei Geschäftsbeziehungen und Transaktionen ohne persönliche Kontakte (Wegleitung zu den Sicherungsmassnahmen nach Art. 14 SPV)

Referenz:	FMA-WL 2019/7
Adressaten:	Sorgfaltspflichtige nach Art. 3 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:	11. Juni 2019
Letzte Änderung:	6. November 2023

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

FMA

Inhalt

1. Hintergrund

Die FMA informiert über ihre Praxis bezüglich Art. 14 Abs. 1 SPV bei Geschäftsbeziehungen und Transaktionen ohne persönliche Kontakte.[1]

Art. 14 Abs. 1 SPV ermöglicht die Kompensation eines fehlenden persönlichen Kontakts[2] bei der Identifikation des Vertragspartners, sofern die in den Ziff. 3 und 4 dieser Wegleitung beschriebenen Sicherungsmassnahmen vom Sorgfaltspflichtigen eingehalten werden.

In diesem Zusammenhang informiert die FMA des Weiteren über ihre Auslegung von Art. 11 Abs. 1 und 2 SPV hinsichtlich der Erfordernisse an die schriftliche Erklärung des Vertragspartners zur Identifizierung der wirtschaftlich berechtigten Person.

Durch die Einhaltung der Sicherungsmassnahmen - welche lediglich Mindestanforderungen darstellen - können potentielle Risiken, die bei einer Identifikation ohne persönlichen Kontakt entstehen können, auf ein Minimum reduziert werden.

Sofern die in den Ziff. 3 und 4 beschriebenen Voraussetzungen erfüllt sind, kann der Sorgfaltspflichtige trotz fehlenden persönlichen Kontakts bei der Identifikation grundsätzlich von einem vergleichbaren Risiko wie bei

[1] Für weitere Informationen iZm Geschäftsbeziehungen und Transaktionen ohne persönliche Kontakte siehe auch die EBA Leitlinien zur Nutzung von Anwendungen für den Fern- Kundenannahmeprozess gemäss Artikel 13 Absatz 1 der Richtlinie (EU) 2015/849 (EBA/GL/2022/15) vom 22. November 2022.

[2] Der Begriff „persönlicher Kontakt“ wird mit „physischer Präsenz“ gleichgestellt.

Geschäftsbeziehungen mit persönlichem Kontakt ausgehen. Weitere Risikofaktoren - insbesondere jene gemäss Anhang 2 Abschnitt A zum SPG - bleiben hiervon jedoch unberührt und können folglich trotz persönlichen Kontakts zu einem erhöhten oder hohen Risiko der betreffenden Geschäftsbeziehung führen.

2. Mögliche Sicherungsmassnahmen

Als Sicherungsmassnahmen im Sinne von Art. 14 Abs. 1 SPV gelten abschliessend:

- Die Anwendung der sog. „Video-Identifikation“;
- Die Anwendung der sog. „Remote-Identifikation“;
- Der Eingang der ersten Zahlung von einem Referenzkonto.

Die genannten Sicherungsmassnahmen dienen der Identifikation natürlicher Personen. Das Vorgehen für Fälle, in denen es sich beim Vertragspartner um einen Rechtsträger handelt, wird in Ziff. 4.3 dieser Wegleitung beschrieben.

3. Allgemeine Ausführungen zu den Sicherungsmassnahmen

3.1. Erforderliche Qualifikation

Die mit dem Identifikationsprozess betrauten Personen müssen über entsprechende Kenntnisse bezüglich des Identifikationsprozesses und der damit verbundenen rechtlichen Anforderungen verfügen. Diese Personen sind durch entsprechende Schulungen auf dem aktuellen Stand der verwendeten Technologien zu halten.

Wird für die Zwecke dieser Wegleitung ein externer Dienstleister herangezogen, so hat der Sorgfaltspflichtige sicherzustellen, dass er die Funktionsweise und Grundlage der Systeme, die dieser Dienstleister verwendet, versteht und somit den Identifikationsprozess nachvollziehen kann. Entsprechende Fragen im Rahmen einer Vor-Ort Kontrolle durch die FMA oder einen beauftragten Wirtschaftsprüfer müssen durch den Sorgfaltspflichtigen selbst beantwortet werden können.

3.2. Datenerhebung

Werden die genannten Sicherungsmassnahmen verwendet, haben die Sorgfaltspflichtigen sicherzustellen, dass ihnen die in Art. 6 Abs. 1 SPV genannten Angaben des Vertragspartners bekannt und im Sorgfaltspflichtakt dokumentiert sind. Es handelt sich hierbei

- bei natürlichen Personen um: Name, Vorname, Geburtsdatum, Wohnsitzadresse, Wohnsitzstaat und Staatsangehörigkeit;
- bei Rechtsträgern um: Name oder Firma, Rechtsform, Sitzadresse, Sitzstaat, Gründungsdatum, gegebenenfalls Ort und Datum des Handelsregistereintrages sowie die Namen der für den Rechtsträger im Verhältnis zum Sorgfaltspflichtigen formell handelnden Organe oder Trustees.

3.3. Erlaubte Identifikationsdokumente

Bei Durchführung der Video- oder Remote-Identifikation von natürlichen Personen dürfen nur diejenigen in Art. 7 SPV genannten beweiskräftigen Dokumente verwendet werden, welche über mind. 2 überprüfbare optisch variable Sicherheitsmerkmale (zB Hologramme, Laserkippbilder) sowie einen maschinenlesbaren Bereich (MRZ) verfügen.

Die Überprüfung der optisch variablen Sicherheitsmerkmale ist in den Fällen, in welchen der Ausweis über einen freigeschalteten RFID-Chip verfügt, primär durch das Auslesen des RFID-Chips zu ersetzen. Die Berechtigungszertifikate sind zu übermitteln und im Sorgfaltspflichtakt abzulegen.[3]

[3] Zu den Berechtigungszertifikaten und deren Dokumentation siehe im Detail unter Pkt. 4.1.2.b.

Bei Rechtsträgern sind die in Art. 8 SPV genannten beweiskräftigen Dokumente (zB Handelsregisterauszug) heranzuziehen.

Die im Rahmen der Video- und Remote-Identifikation erstellten Videos bzw. Fotos des Identifikationsdokuments und der zu identifizierenden Person gelten als vollwertiger Ersatz für die Einsichtnahme in ein beweiskräftiges Dokument im Sinne von Art. 6 ff. SPV.

3.4. Dokumentation

Der Sorgfaltspflichtige hat die Anwendung von Sicherungsmassnahmen für Geschäftsbeziehungen und Transaktionen ohne persönliche Kontakte in seine internen Weisungen gemäss Art. 31 SPV aufzunehmen. Insbesondere sind die verwendeten Sicherungsmassnahmen und die laufende Erfüllung der Voraussetzungen, die sich aus Art. 14 SPV iVm der gegenständlichen Wegleitung ergeben, zu beschreiben. Ausserdem sind mögliche Auswirkungen auf die unternehmensweite Risikobewertung zu beurteilen. Die Kundenkategorien bei denen Geschäftsbeziehungen und Transaktionen ohne persönlichen Kontakt (unter Einhaltung der erforderlichen Sicherungsmassnahmen) aufgenommen bzw. durchgeführt werden dürfen, sind ebenfalls in den internen Weisungen zu beschreiben.

Die beschriebenen Voraussetzungen zur Anwendung der jeweiligen Sicherungsmassnahme sind kumulativ zu erfüllen. Ihr Vorliegen ist zu dokumentieren und das Ergebnis der einzelnen Prüfschritte sowie das Gesamtergebnis des Identifikationsprozesses sind im Sorgfaltspflichtakt abzulegen.

Es sind sämtliche im Rahmen der Identifikation erstellten Dokumente und Aufzeichnungen zum jeweiligen Sorgfaltspflichtakt zu nehmen.

Sie sind nach Massgabe der in Art. 20 SPG genannten Fristen aufzubewahren. Dies beinhaltet auch die LOG-Files (Protokolldateien) sowie den gesamten „Videostream“ (im Falle von Video-Identifikation), welche im Rahmen der Identifikation erstellt werden. Sämtliche Dateien müssen dabei in einer Qualität aufbewahrt werden, die es einem fachkundigen Dritten im Sinne von Art. 28 Abs. 1 Bst. b SPV ermöglicht, die Einhaltung der Vorgaben dieser Wegleitung zu prüfen.

3.5. Vorgehen bei Unstimmigkeiten

Im Fall von Übertragungsschwierigkeiten ist der Identifikationsprozess abzubrechen. Dies gilt für Fälle, in denen beispielsweise die Qualität der Internetverbindung oder die vorherrschenden Lichtverhältnisse eine ordnungsgemässe Identifikation verunmöglichen.

Beim Vorliegen von Unstimmigkeiten oder Unsicherheiten wie beispielsweise im Falle von erkennbaren Manipulationen am Identifikationsdokument, ist der Identifikationsprozess zwar nicht abzubrechen, aber zu vermerken, dass die Identifikation nicht erfolgreich war. In einem solchen Fall gelangt Art. 5 Abs. 3 Bst. a SPG zur Anwendung und die gegenständliche Geschäftsbeziehung darf nicht aufgenommen bzw. die gewünschte Transaktion nicht durchgeführt werden.

Es ist in diesem Zusammenhang ebenfalls die in Art. 17 SPG statuierte Pflicht zur Erstattung einer Mitteilung an die Stabsstelle FIU zu beachten. Diesbezüglich wird auf die entsprechenden Ausführungen in der „FMA-Wegleitung 2018/7 – Allgemeine und branchenspezifische Auslegung des Sorgfaltspflichtrechts“ verwiesen.

3.6. Verhältnis zu weiteren sorgfaltspflichtrechtlichen Bestimmungen

Die weiteren Bestimmungen aus SPG und SPV, insbesondere hinsichtlich der Pflichten zur Erstellung des Geschäftsprofils sowie zur risikoadäquaten Überwachung der Geschäftsbeziehung nach Art. 5 Abs. 1 Bst. c und d SPG bleiben von den Ausführungen in dieser Wegleitung gänzlich unberührt.

Dasselbe gilt hinsichtlich Art. 18 SPV, der besagt, dass alle für die Feststellung und Überprüfung der Identität des Vertragspartners und der wirtschaftlich berechtigten Person erforderlichen Angaben und Dokumente vollständig und in gehöriger Form bei Aufnahme der Geschäftsbeziehung oder Abwicklung einer gelegentlichen Transaktion vorliegen müssen. Insbesondere bleiben die in Art. 18 Abs. 2 und 3 SPV genannten Ausnahmen von diesem Grundsatz unter Einhaltung der dort beschriebenen Voraussetzungen anwendbar.

4. Die Sicherungsmassnahmen

4.1. Anwendung der sog. „Video-Identifikation“

Diese Art der Identifikation ist bei natürlichen Personen, die als Vertragspartner auftreten, zulässig, sofern nachfolgende Punkte kumulativ eingehalten werden:

4.1.1. Audiovisuelle Wahrnehmung

Bei Nutzung der Video-Identifikation muss die audiovisuelle Kommunikation mit dem Vertragspartner gewährleistet sein. Es ist daher zwingend eine Videoübertragung in Echtzeit vorzunehmen. Die Aufnahme muss durch die Hardware (Kamera) des Vertragspartners vorgenommen und direkt im Laufe des Identifikationsprozesses erstellt werden.

Die Videoübertragung ist nach dem aktuellen Stand der Technik zu verschlüsseln. Die Qualität des genutzten Streams muss derart sein, dass die nachfolgenden Prüfschritte durchgeführt werden können.

4.1.2. Durchführung der Identifikation

Es sind/ist:[4]

a) per Videochat sowohl das Gesicht des Vertragspartners als auch Vorder- und Rückseite der relevanten Datenseite des Identifikationsdokuments sichtbar zu erfassen. Dabei ist sicherzustellen, dass das Video direkt im Laufe des Identifikationsprozesses erstellt wird.

   Konkret sind Vorkehrungen zu treffen, die ausschliessen, dass im Video eine fremde oder eine nicht lebende Person auftritt. Dies kann beispielsweise dadurch erreicht werden, dass dem Vertragspartner im Rahmen des Anmelde-/Identifikationsprozesses konkrete Bewegungsabläufe vorgegeben werden, die sie vorzunehmen hat. Dabei ist durch Anwendung des Zufallsprinzips sicherzustellen, dass diese Vorgaben wechseln und nicht bei jeder Identifikation dieselben sind.

   Sofern einzelne Angaben auf dem Identifikationsdokument nicht erkennbar sind, ist der Vorgang zu wiederholen.

   Ein Screenshot der Vorder- und Rückseite des Identifikationsdokuments sind zum Sorgfaltspflichtakt zu nehmen.

b) das Identifikationsdokument auf das Vorhandensein mindestens zweier optisch variabler Sicherheitsmerkmale (zB Hologramme, Laserkippbilder) zu prüfen. Im Video-Stream müssen die Effekte dieser Sicherheitsmerkmale in ihren unterschiedlichen Zuständen ersichtlich sein (beispielsweise einmal sichtbar und einmal nicht sichtbar); diesbezüglich ist insbesondere darauf zu achten, dass die Lichtverhältnisse ausreichend sind.

   Sofern die Prüfung der optisch variablen Sicherheitsmerkmale durch das Auslesen des RFID-Chips mittels NFC-Technologie ersetzt wird, sind insbesondere die Zertifikate des Ausstellers (Document Signer Certificate; CSCA-Certificate/ICAO) sowie des Ausweises selbst (Certificate Revocation List) im Rahmen des Identifikationsprozesses auf deren Gültigkeit hin zu überprüfen. Nach Abschluss der Überprüfung der Berechtigungszertifikate sind diese im Sorgfaltspflichtakt abzulegen. Wird die Überprüfung der Berechtigungszertifikate durch einen Dritten durchgeführt, kann anstelle der Berechtigungszertifikate selbst, die Bestätigung der durchgeführten Überprüfung im Sorgfaltspflichtakt abgelegt werden. Diesfalls ist vom Sorgfaltspflichtigen sicherzustellen, dass eine Bestätigung des Dritten nur im Falle einer positiven Überprüfung der Berechtigungszertifikate ausgestellt wird.[5]

c) zu prüfen, ob das Ausstellungs- und Gültigkeitsdatum des Identifikationsdokuments plausibel sind, beispielsweise, dass das Ausstellungsdatum vor dem Gültigkeitsdatum liegt und dass beide Daten nach dem Geburtsdatum liegen. Ferner darf die Gültigkeitsdauer des vorgelegten Ausweisdokumentes nicht gegen die für Ausweisdokumente dieser Art geltende Norm verstoßen.

[4] In Fällen, in denen das Auslesen des RFID-Chips angewendet wird, entfallen die Vorgaben in den Bst. d), e) und f).
[5] Dies ist nachweislich (z.B. vertraglich) sicherzustellen und zu dokumentieren.

d) durch eine automatisierte Berechnung, welche beispielsweise durch Nutzung der „Optical Character Recognition“ (OCR-Auslesung) erreicht werden kann, sicherzustellen, dass die in der maschinenlesbaren Zone enthaltenen Daten mit den auf dem Identifikationsdokument enthaltenen Daten übereinstimmen, sowie, dass die verwendete Ziffernorthographie und die Schriftart korrekt sind.

e) in Fällen, in denen der Identifizierende mit dem Identifikationsdokument nicht vertraut ist, ein Abgleich mit einer Ausweisdatenbank wie zB PRADO oder einer gleichwertigen Datenbank vorzunehmen. Sofern ein Abgleich mit einer Ausweisdatenbank nicht im Prozess selbst durchgeführt werden kann, ist der Identifikationsvorgang abzubrechen. In jenen Fällen, in welchen das Ausweisdokument nicht in lateinischen Schriftzeichen verfasst ist, sind entsprechende Übersetzungen im Sorgfaltspflichtakt zu dokumentieren.

f) das Identifikationsdokument auf erkennbare Beschädigungen bzw. Manipulationen zu prüfen.

g) das Bild des Identifikationsdokuments mit dem Vertragspartner abzugleichen. Die FMA empfiehlt, den Abgleich durch Verwendung eines elektronischen biometrischen Verfahrens durchzuführen, dessen „False Acceptance Rate“[6] kleiner als 1 % ist.

h) die Stimmigkeit bereits vorhandener Daten mit den Angaben des Vertragspartners zu prüfen. Hierzu sind der zu identifizierenden Person im Gespräch entsprechende psychologische Fragen beispielsweise zu vorab gesammelten oder auf dem Identifikationsdokument vorhandenen Daten zu stellen oder auch um den Zweck der Identifikation zu hinterfragen.

i) die Korrektheit der angegebenen Daten nach erfolgter Erfassung aller notwendigen Informationen durch die zu identifizierende Person zu bestätigen. Dies kann beispielsweise durch Verwendung einer einzig für diesen Zweck generierten, individuellen TAN oder entsprechende mündliche Bestätigung erreicht werden.

Aus Gründen des Datenschutzes empfiehlt es sich zudem, den Identifikationsprozess in einem separaten und mit einer Zugangskontrolle ausgestatteten Raum vorzunehmen.

4.1.3. Plausibilisierungsmassnahmen nach Durchführung der Identifikation

Während oder im direkten Anschluss an die Identifikation sind Plausibilisierungsmassnahmen hinsichtlich der geographischen Merkmale vorzunehmen. Diesbezüglich ist sicherzustellen, dass das Ergebnis hinsichtlich der Geolokation der IP-Adresse auch mit den Angaben zum Wohnsitz oder zum Arbeitsplatz der identifizierten Person übereinstimmt. Sofern diesbezüglich keine Übereinstimmung besteht oder Hinweise dahingehend vorliegen, dass seitens der identifizierten Person Massnahmen zur Verschleierung des Standorts getroffen wurden (VPN, TOR-Browser etc.), sind Abklärungen durchzuführen. Dazu gehört beispielsweise die Einholung einer aktuellen «utility bill», der Abgleich mit der Steuernummer oder die Durchführung einer Ersttransaktion[7] von einem Bankkonto (sog. Referenzkonto) aus dem als Wohnsitz angegebenen Land. Sofern die Adress- und Lokalisationsdaten nicht übereinstimmen und die Abklärung nicht plausibel ausfällt, darf in der Folge eine Geschäftsbeziehung nur dann eröffnet werden, wenn eine restlose Klärung des Sachverhaltes vorgenommen werden konnte oder allenfalls verstärkte Sorgfaltspflichten zur Anwendung kommen.

4.2. Anwendung der sog. „Remote-Identifikation“

In Fällen, in denen es sich beim Vertragspartner um eine natürliche Person handelt, kann als Alternative zur Video-Identifikation eine elektronische Identifikation erfolgen, bei welcher nicht zwingend ein direkter Kontakt in Echtzeit zwischen Sorgfaltspflichtigem und der zu identifizierenden Person besteht. Diese Art der Identifikation ist zulässig, sofern nachfolgende Punkte kumulativ eingehalten werden.

[6] Unter der „False Acceptance Rate“ versteht die FMA die generelle Fehleranfälligkeit der Software bzw. die Wahrscheinlichkeit der Software, eine falsche Beurteilung abzugeben. Hiervon zu unterscheiden ist der finale Entscheid des Sorgfaltspflichtigen, ob die Identifikation als erfolgreich durchgeführt angesehen wird oder nicht.

[7] Die erste Transaktion auf dem neu eröffneten Konto muss von einem Bankkonto (sog. Referenzkonto) aus dem vom Vertragspartner angegebenen Wohnsitzland eingehen, bei dem es sich nachweislich um ein Einzel- oder Gemeinschaftskonto des betreffenden Vertragspartners handelt.

Es sind/ist:

a) Fotos der Vorder- und Rückseite der Datenseite eines der in Art. 7 SPV genannten, beweiskräftigen Identifikationsdokumente anzufertigen und zum Sorgfaltspflichtakt zu nehmen.

   Das Identifikationsdokument im Sinne von Ziff. 4.1.2. Bst. b) bis f) dieser Wegleitung durch den Sorgfaltspflichtigen zu prüfen. Es ist entsprechend dem aktuellen Stand der Technik sicherzustellen, dass Beschädigungen, Fälschungen oder Manipulationen von Ausweisdokumenten erkannt werden.

b) ein Foto der zu identifizierenden Person anzufertigen. Hierbei ist nach Ziff. 4.1.2. Bst. a) zu verfahren.

c) die Fotografie des Identifikationsdokuments mit der zu identifizierenden Person abzugleichen. Hierbei ist zwingend ein Abgleich durch Verwendung eines elektronischen biometrischen Verfahrens nach Ziff. 4.1.2. Bst. g) durchzuführen.

d) die Korrektheit der angegebenen Daten nach erfolgter Erfassung aller notwendigen Informationen durch die zu identifizierende Person zu bestätigen (analog Ziff. 4.1.2. Bst. i)).

e) der Identifikationsvorgang nach dem aktuellen Stand der Technik zu verschlüsseln.

f) Plausibilisierungsmassnahmen wie in 4.1.3 vorgegeben durchzuführen.

4.3. Zusätzliche Voraussetzungen bei der Identifikation von Rechtsträgern als Vertragspartner im Sinne des SPG

Sofern es sich beim Vertragspartner um einen Rechtsträger handelt, müssen die Vorgaben des Art. 6 SPG in Verbindung mit Art. 6 Abs. 1 Bst. b und Art. 8 ff. SPV eingehalten werden.

Da Art. 6 Abs. 1 Bst. b i.V.m. Abs. 3 SPV auf die für den Rechtsträger handelnden natürlichen Personen abstellt, müssen diese im Rahmen der Video- oder Remote-Identifikation gegenüber dem Sorgfaltspflichtigen auftreten. Aus diesem Grund muss auch die für den Rechtsträger handelnde Person sowie deren Identifikationsdokument im Sinne der Vorgaben dieser Wegleitung zur Video- oder Remote Identifikation geprüft und dokumentiert werden.

Dabei ist es dem Sorgfaltspflichtigen freigestellt, ob er das nach Art. 6 Abs. 1 Bst. b und Art. 8 SPV erforderliche, beweiskräftige Identifikationsdokument des Rechtsträgers auf geeignete Weise selbständig einholt (zB schriftlicher Auszug aus einer öffentlich zugänglichen Datenbank des Handelsregisters) oder es sich vom Rechtsträger separat zukommen lässt.

Sofern in letzterem Fall eine elektronische Übermittlung erfolgen soll, so ist das Identifikationsdokument des Rechtsträgers nach Art. 8 SPV (zB Handelsregisterauszug) als Scan/Foto vom Original zu übermitteln, sofern die folgenden Voraussetzungen erfüllt sind:

a) eine Echtheitsbestätigung durch die in Art. 9 SPV genannten Sorgfaltspflichtigen am Identifikationsdokument vorgenommen wird;

b) die Vorgaben des Art. 10 Abs. 3 SPV hinsichtlich der Aktualität der Dokumente eingehalten werden; und

c) das Identifikationsdokument unter Verwendung einer sicheren elektronischen Signatur nach Art. 2 Abs. 1 Bst. d oder Art. 24 Abs. 3 des Signaturgesetzes (SigG) vom Vertragspartner an den Sorgfaltspflichtigen übermittelt wird und das gescannte Identifikationsdokument untrennbar mit dieser sicheren elektronischen Signatur verbunden ist.

4.4. Identifikation über eine eingehende Zahlung von einem Referenzkonto

In Fällen, in denen nach Art. 10 SPG vereinfachte Sorgfaltspflichten angewandt werden dürfen, kann die Identifikation einer natürlichen Person als Vertragspartner auch dadurch erfolgen, dass die erste Transaktion auf dem neu eröffneten Konto von einem Bankkonto (sog. Referenzkonto) aus dem EWR-Raum oder der Schweiz eingeht, bei dem es sich nachweislich um ein Einzel- oder Gemeinschaftskonto des betreffenden Vertragspartners handelt.

Der Sorgfaltspflichtige hat sich auf geeignete Weise davon zu überzeugen, dass es sich beim Inhaber des Kontos, von welchem diese erste Zahlung ausgeht, tatsächlich um den gegenständlichen Vertragspartner handelt und in der Folge zu überprüfen, dass die erste Überweisung auch von diesem Konto aus eingeht.

Hierbei können die mit der Transaktion übermittelten Daten ausreichend sein, sofern sich daraus zweifelsfrei ergibt, dass es sich beim Auftraggeber und Kontoinhaber der Zahlung um den Vertragspartner handelt. Es kann hierbei allerdings auch auf anderweitige Unterlagen wie Kontoauszüge oder ähnliches zurückgegriffen werden.

Das entsprechende Konto beim Sorgfaltspflichtigen ist unter Anwendung von Art. 18 Abs. 2 SPV jedenfalls bis zum vollständigen Abschluss des Identifikationsvorganges und des Einlangens der entsprechenden Zahlung für ausgehende Transaktionen zu sperren. Der Sorgfaltspflichtige hat in der Folge zu überprüfen, dass die erste Überweisung von dem gegenständlichen Referenzkonto aus eingeht.

5. Erklärung des Vertragspartners zur Identität der wirtschaftlich berechtigten Person

Nach Art. 11 Abs. 2 SPV hat der Vertragspartner oder eine durch diesen bevollmächtigte Person gegenüber dem Sorgfaltspflichtigen die Richtigkeit der Angaben zur Identität der wirtschaftlich berechtigten Person zu bestätigen durch

a) Unterschrift oder

b) durch ein anderes gleichwertiges Verfahren, bei dem:

1. der Vertragspartner oder eine durch diesen bevollmächtigte Person eindeutig identifiziert wird; und
2. die Integrität der Angaben und deren Authentifikation durch den Vertragspartner gewährleistet ist.

Die weiteren Pflichten nach Art. 7 bis Art. 7b SPG bleiben von dieser Erklärung unberührt.

Als Unterschrift des Vertragspartners gelten nach Auffassung der FMA auch eigenhändige Unterschriften, die nachweislich durch den Vertragspartner im Identifizierungsprozess selbst auf einem dafür technisch geeigneten Gerät wie beispielsweise einem Tablet vorgenommen werden. In einem solchen Fall ist das Erfordernis der „Schriftlichkeit“ der Erklärung des Vertragspartners als erfüllt zu betrachten.

Alternativ kann die Einholung dieser Bestätigung vom Vertragspartner wie bisher im Rahmen der Video-Identifikation erfolgen. Dabei muss das relevante Formular direkt im Rahmen des Videochats vom Vertragspartner vor den Augen des Sorgfaltspflichtigen bzw. des betrauten Mitarbeiters unterzeichnet werden. Die Aufzeichnung dieses Vorgangs ist wiederum zum Sorgfaltspflichtakt zu nehmen.

Als gleichwertiges Verfahren im Sinne von Art. 11 Abs. 2 Bst. b SPV gilt beispielsweise die Erhebung der notwendigen Daten und die Durchführung der Identifikation des Vertragspartners mit anschliessender Bestätigung durch Verwendung einer individuellen TAN. Dabei ist darauf zu achten, dass für jeden Bestätigungsvorgang, wobei dieser nicht ausschliesslich der Bestätigung der Identität der wirtschaftlich berechtigten Person dienen muss, ein neuer TAN generiert wird.

Als gleichwertiges Verfahren im Sinne von Art. 11 Abs. 2 Bst. b SPV gilt auch die Unterzeichnung mittels einer «qualifizierten elektronischen Signatur» gemäss Signatur- und Vertrauensdienstgesetz.

6. Delegation und Outsourcing

Sofern der Sorgfaltspflichtige im Rahmen der Video- oder Remote-Identifikation auf einen externen Dienstleister, wie beispielsweise ein auf die Durchführung der Identifikation spezialisiertes Unternehmen bzw. einen sog. KYC-Dienstleister zurückgreift, müssen in jedem Fall die Voraussetzungen des Art. 24a Abs. 1a SPV bzw. im Falle der Delegation an einen anderen Sorgfaltspflichtigen des Art. 14 SPG i.V.m. Art. 24 SPV erfüllt sein.

Wird für die Identifikation des Vertragspartners ein externer Dienstleister verwendet, so kann dieser, sofern er die betreffende Person bereits für einen anderen Sorgfaltspflichtigen nach den liechtensteinischen sorgfaltspflichtrechtlichen Vorgaben identifiziert hat, auf diese Dokumentation zurückgreifen. Die Aktualität der

vorhandenen Daten im Sinne des SPG und der SPV ist in jedem Fall zu prüfen und gegebenenfalls durch erneutes Einholen beispielsweise eines Registerauszugs, der nicht älter als 12 Monate ist (Art. 10 Abs. 3 SPV), sicherzustellen.

Zu beachten bleibt, dass der in Anspruch genommene externe Dienstleister die ihm übertragenen Aufgaben nicht auf einen Dritten übertragen darf (Art. 24 Abs. 3 SPV; Art. 24a Abs. 1a Bst. d SPV). Im Übrigen wird auf die Ausführungen zur Delegation und zum Outsourcing in der FMA-WL 2018/7 verwiesen.

7. 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.

8. Schlussbestimmungen

8.1. Inkrafttreten

Diese Wegleitung tritt mit 11. Juni 2019 in Kraft.

Die Änderungen vom 12. März 2020 traten am selben Tag in Kraft.

Die Änderungen vom 6. November 2023 treten am 6. Mai 2024 in Kraft.

Stand: 6. November 2023

9. Änderungsverzeichnis

Am 12. März 2020 wurden folgende Anpassungen vorgenommen:

- **Ziff. 4.2. Anwendung der sog. „Remote-Identifikation“**

  Unter Bst. c wurde klargestellt, dass die Remote-Identifikation zwingend die Verwendung eines elektronischen biometrischen Verfahrens bedarf.

- **Ziff. 5 Erklärung des Vertragspartners zur Identität der wirtschaftlich berechtigten Person**

  Die Ausführungen wurden an die Änderungen der SPV zum 1. Januar 2020 angepasst, sodass in Zukunft eine eigenhändige Unterschrift nicht mehr erforderlich ist, sofern die Voraussetzungen des Art. 11 Abs. 2 Bst. b SPV eingehalten sind. Damit wurde die Aufnahme von Geschäftsbeziehungen ohne Medienbruch ermöglicht.

Am 6. November 2023 wurden folgende Anpassungen vorgenommen:

- **Ziff. 1 FN 1, Ziff. 3.1 und Ziff. 3.4 notwendige Ergänzungen, die sich aufgrund der EBA Leitlinien zur Nutzung von Anwendungen für den Fern- Kundenannahmeprozess gemäss Artikel 13 Absatz 1 der Richtlinie (EU) 2015/849 (EBA/GL/2022/15) vom 22. November 2022 ergeben.**

  Bei Verwendung der gegenständlichen Sicherungsmassnahmen sind die damit betrauten Mitarbeiter entsprechend zu schulen. Ausserdem hat der Sorgfaltspflichtige die Anwendung von Sicherungsmassnahmen für Geschäftsbeziehungen und Transaktionen ohne persönliche Kontakte in seine internen Weisungen aufzunehmen.

- **Ziff. 3.3 und Ziff. 4.1.2 Bst. b Einführung der Verpflichtung zum Auslesen des RFID-Chips mittels NFC**

  Die Überprüfung der optisch variablen Sicherheitsmerkmale sollte in Fällen, in denen ein entsprechendes Ausweisdokument vorhanden ist, primär durch das Auslesen des RFID-Chips erfolgen.

- **Ziff. 4.1.3 Verpflichtung zu Plausibilisierungsmassnahmen hinsichtlich Geolokation/Wohnsitzadresse**

  Stimmt der Datenabgleich zwischen Geolokation der IP-Adresse nicht mit den Angaben zum Wohnsitz oder zum Arbeitsplatz überein, sind weitere Abklärungen durchzuführen.

- **Ziff 4.2 Bst. a Einführung einer Fälschungsprüfung**

  Im Rahmen der Anwendung von Sicherungsmassnahmen sind die verwendeten Ausweisdokumente auf mögliche Fälschungen zu überprüfen.

- **Ziff. 5 Aufnahme der «qualifizierten elektronischen Signatur» als gleichwertiges Verfahren**

  Die Unterzeichnung mittels «qualifizierter elektronischer Signatur» gemäss Signatur- und Vertrauensdienstgesetz wird als gleichwertiges Verfahren im Sinne von Art. 11 Abs. 2 Bst. b SPV anerkannt.