Begründung

Allgemeiner Teil

Ist ein potentieller Kunde oder dessen vertretungsbefugte natürliche Person für die Feststellung und Überprüfung seiner Identität nicht beim Verpflichteten physisch anwesend und ist daher die persönliche Vorlage eines amtlichen Lichtbildausweises im Sinne des § 6 Abs. 2 Z 1 Finanzmarkt-Geldwäschegesetz – FM-GwG, BGBl. I Nr. XX/2016, nicht möglich, bildet dies einen Faktor für ein potentiell erhöhtes Risiko, wenn keine weiteren bestimmten Sicherungsmaßnahmen gesetzt werden (Anlage III zu § 9 FM-GwG). Daher kann auch gemäß § 6 Abs. 4 FM-GwG die persönliche Vorlage des amtlichen Lichtbildausweises nur dann durch eine Vorlage im Rahmen eines videogestützten elektronischen Verfahrens (Online-Identifikation) ersetzt werden, wenn das erhöhte Risiko durch entsprechende Sicherungsmaßnahmen ausgeglichen wird. Nach dieser Bestimmung ist die FMA deswegen zugleich berechtigt und verpflichtet mit Verordnung festzulegen, welche Sicherungsmaßnahmen zum Ausgleich des erhöhten Risikos erforderlich sind. Dabei bedarf diese Verordnung der Zustimmung des Bundesministers für Finanzen. Diesem Regelungsauftrag soll mit dieser Verordnung nachgekommen werden.

Durch die in dieser Verordnung festgelegten Sicherungsmaßnahmen soll insbesondere sichergestellt werden, dass die Beteiligten an der Identifikation visuell wahrnehmbar sind, eine gleichzeitige sprachliche Kontaktaufnahme möglich ist, die Identität des potentiellen Kunden oder der vertretungsbefugten natürlichen Person des Kunden anhand eines Identifikationsdokumentes festgestellt werden kann und dabei die mit einer Fernkommunikation einhergehenden Unsicherheiten ausgeglichen werden.

Die Verordnung erfüllt mit den in ihr enthaltenen Sicherungsmaßnahmen außerdem den Verordnungsauftrag, insbesondere Anforderungen an die Datensicherheit, Fälschungssicherheit und an jene Personen, die die Online-Identifikation durchführen, festzulegen, soweit diese abgeleiteten Anforderungen dem Hauptziel dienen, einen Ausgleich für das potentiell erhöhte Risiko der Geldwäscherei und Terrorismusfinanzierung im Rahmen der Online-Identifikation zu gewährleisten. Enthalten sind diese Sicherungsmaßnahmen in den organisatorischen Bestimmungen des § 3.

Besonderer Teil

Zu § 1:

Die Bestimmung regelt den Gegenstand dieser Verordnung, nämlich erforderliche Sicherungsmaßnahmen für die Online-Identifikation festzulegen. Dabei wird durch Abs. 2 klargestellt, dass die durch die gegenständliche Verordnung festgelegten Sicherungsmaßnahmen keine der Sorgfaltspflichten des FM-GwG zur Prävention von Geldwäscherei und Terrorismusfinanzierung verdrängen. Vielmehr werden durch die Verordnung solche Sicherungsmaßnahmen für die Online-Identifikation festgelegt, die verstärkte Sorgfaltspflichten für Geschäftsbeziehungen, die auf diese Art begründet werden, grundsätzlich vermeiden sollen. Unbeschadet dessen steht es jedem Verpflichteten frei, zusätzliche Sicherungsmaßnahmen zu implementieren, um das Schutzniveau zur Prävention von Geldwäscherei und Terrorismusfinanzierung weiter zu erhöhen.

Die Online-Identifikation stellt eine Verarbeitung von Daten gemäß § § 4 Z 9 des Datenschutzgesetzes 2000 – DSG 2000, BGBl. I Nr. 165/1999, in der Fassung des Bundesgesetzes BGBl. I Nr. 83/2013 und der Kundmachung BGBl. I Nr. 132/2015 dar. Dementsprechend wird in Abs. 4 klargestellt, dass sich für das Verfahren der Online-Identifikation weitere Vorgaben aus dem DSG 2000 ergeben. In § 4 Abs. 2 und § 6 Abs. 1 wird lediglich zur Verdeutlichung ausdrücklich klargestellt, dass die §§ 11 und 50a Abs. 5 DSG 2000 anzuwenden sind.

Zu § 2:

Für die Zwecke dieser Verordnung werden zwei Begriffe, derjenige der Bildschirmkopie und derjenige des amtlichen Lichtbildausweises näher bestimmt.

Die Bildschirmkopie definiert einen Rechtsbegriff, der dem im Alltagsgebrauch verwendeten Begriff des „Screenshot“ vergleichbar ist. Die Bildschirmkopie steht graphisch reproduzierbar für die visuelle Komponente der Online-Identifikation zu einem bestimmten Zeitpunkt, die sich einerseits von der ebenfalls geregelten und reproduzierbaren akustischen Komponente der Online-Identifikation und andererseits von der die gesamte Zeitspanne des Vorganges der Online-Identifikation umfassenden audio-visuellen Komponente abgrenzt. Dabei ist die Videodokumentation ein Beispiel für eine Sicherungsmaßnahme, die weder von dieser Verordnung gefordert, noch von ihr verboten wird und die jedenfalls als freiwillige

Maßnahme das Schutzniveau zur Prävention von Geldwäscherei und Terrorismusfinanzierung weiter erhöhte.

Der amtliche Lichtbildausweis ist zunächst in § 6 Abs. 2 Z 1 FM-GWG definiert. Soweit für die Zwecke dieser Verordnung eine einengende Begriffsdefinition durch ein weiteres Begriffsmerkmal vorgenommen wird, geschieht dies zum Ausgleich des erhöhten Risikos der Geldwäscherei und Terrorismusfinanzierung, das mit einer Online-Identifikation einhergeht. Konkret werden bei Lichtbildausweisen optische Sicherheitsmerkmale gefordert, welche im Vergleich zu holographischen Sicherheitsmerkmalen zumindest gleichwertig sind. Diese Vorgabe korrespondiert mit der Verfahrenspflicht für den betroffenen Mitarbeiter des Verpflichteten oder des Dienstleisters (§ 6 Abs. 1), die Authentizität eines Lichtbildausweises unter anderem zu prüfen, indem dessen holographische Sicherheitsmerkmale im Zuge seines horizontalen und vertikalen Kippens überprüft werden sollen (§ 4 Abs. 4 Z 1).

Zu § 3:

Die Bestimmung regelt die erforderlichen organisatorischen Sicherungsmaßnahmen.

Wie aus dieser Verordnung sowie ihrer gesetzlichen Grundlage selbst hervorgeht, ist die Online-Identifikation mit einem besonderen rechtlichen Rahmen verbunden. Dabei darf nicht vergessen werden, dass es sich bei der Online-Identifikation um eine Datenverarbeitung gemäß § 4 Z 9 DSG 2000 handelt. Darüber hinaus findet die Online-Identifikation im Rahmen der Fernkommunikation statt, an die zum Zwecke der Prävention von Geldwäscherei und Terrorismusfinanzierung besonders hohe technische Anforderungen gestellt werden. Beispielhaft seien genannt die Möglichkeit und tatsächliche Anfertigung einer Bildschirmkopie (§ 4 Abs. 1) oder die Prüfung der technischen Voraussetzungen, unter denen eine Online-Identifikation durchgeführt werden kann oder gemäß § 5 Z 1 abgebrochen werden muss. Schließlich ist eine rechtlich zulässige und technisch beherrschte Durchführung einer Online-Identifikation durch den Mitarbeiter des Verpflichteten oder des Dienstleisters (§ 6 Abs. 1) nur Mittel zum Zwecke der Prävention von Geldwäscherei und Terrorismusfinanzierung. Deswegen muss der Mitarbeiter auch praktisch, z. B. anhand von Rollenspielen oder Best Practice, mit dem Ziel geschult werden, dass er tatsächlich den vom Gesetz intendierten Zweck der Prävention von Geldwäscherei und Terrorismusfinanzierung sicherstellen kann. Zusätzlich müssen die Mitarbeiter, die mit der Durchführung der Online-Identifikation beim Verpflichteten oder Dienstleister (§ 6 Abs. 1) betraut werden, die entsprechende persönliche Zuverlässigkeit aufweisen.

Das in dieser Verordnung geregelte Verfahren der Online-Identifikation soll Gefahren der Geldwäscherei und Terrorismusfinanzierung minimieren, ohne dass hierfür Abstriche bei den Anforderungen an eine verantwortungsvolle Unternehmensführung (Governance) im Übrigen – sowohl aus der Sicht der Prävention von Geldwäscherei und Terrorismusfinanzierung als auch aus umfassenderer Unternehmenssicht – hingenommen werden. Deswegen hat der Verpflichtete sicherzustellen, dass die im Rahmen der Online-Identifikation herangezogenen Anwendungen sowie die übertragenen Daten zu keinem Konflikt mit anderen Prozessen führen, eine das Identifizierungsergebnis verfälschende Beeinflussung des Vorgangs der Online-Identifikation ausgeschlossen ist und die Anwendungen sowie die Daten vor einem unbefugten Zugriff geschützt sind. Eine technische Zertifizierung der verwendeten Anwendungen und angewandten Prozesse als unbedenklich im Hinblick auf die angesprochenen IT-Risiken kann hierfür sinnvoll sein, ohne dass dies durch diese Verordnung verbindlich vorgegeben würde.

Im Rahmen der Fernkommunikation muss die Kontrolle, wer beteiligt ist, stärker als bei der Kommunikation unter physisch Anwesenden technisch gewährleistet werden. Deswegen darf die Online-Identifikation von Mitarbeitern des Verpflichteten ebenso wie von Mitarbeitern eines Dienstleisters (§ 6 Abs. 1) nur in einem abgetrennten, mit Zugangskontrolle ausgestatteten Raum durchgeführt werden.

Zu § 4:

Die Bestimmung regelt die erforderlichen verfahrensbezogenen Sicherungsmaßnahmen.

Einleitend wird der datenschutzrechtliche Rahmen klargestellt. Gemäß § 21 Abs. 4 FM-GwG dürfen personenbezogene Daten von Verpflichteten ausschließlich auf Grundlage des FM-GwG für die Zwecke der Verhinderung von Geldwäscherei und Terrorismusfinanzierung und nicht für andere Zwecke verarbeitet werden. Diese ausdrückliche gesetzliche Ermächtigung im Sinne von § 8 Abs. 1 Z 1 DSG 2000 erstreckt sich auch auf die Online-Identifikation gemäß § 6 Abs. 4 FM-GwG, wie sie durch diese Verordnung mit Zustimmung des Bundesministers für Finanzen näher spezifiziert wird. Deswegen gilt auch, dass die Informationspflicht gemäß § 21 Abs. 5 FM-GwG bei der Begründung einer neuen Geschäftsbeziehung u. a. gilt, worauf hier ausdrücklich hingewiesen werden soll.

Für die Telefonaufzeichnung und die Bildschirmkopien gelten die Aufbewahrungs- und Löschungspflichten gemäß § 21 Abs. 1 und 2 FM-GwG; sie werden durch diese Verordnung nicht aufgrund von § 21 Abs. 3 FM-GwG verlängert. Grund der Telefonaufzeichnung und ihrer Aufbewahrung ist es, dass

der FMA damit die Möglichkeit eingeräumt wird, die Einhaltung der erforderlichen Sicherungsmaßnahmen bei der Online-Identifikation, wie sie sich aus der gegenständlichen Verordnung ergeben, durch die Verpflichteten zu überprüfen. Wird für die Feststellung und Überprüfung der Identität von natürlichen Personen das Verfahren der Online-Identifikation verwendet, sind über die Sorgfaltspflichten des FM-GwG hinaus zusätzliche Sicherungsmaßnahmen anzuwenden, um das potentiell erhöhte Risiko, das sich aus der fehlenden physischen Anwesenheit ergeben kann, auszugleichen. Damit die FMA auch die Einhaltung dieser zusätzlichen Sicherungsmaßnahmen – dies betrifft insbesondere die verfahrensbezogenen Sicherungsmaßnahmen des § 4 – überprüfen kann, ist es notwendig, dass auch das Telefongespräch aufgezeichnet wird. Nur dadurch kann im Zuge einer Überprüfung der FMA zum Beispiel festgestellt werden, ob der Mitarbeiter, der die Online-Identifikation durchgeführt hat, die natürliche Person dazu aufgefordert hat, den amtlichen Lichtbildausweis entsprechend § 4 Abs. 4 Z 1 horizontal und vertikal zu kippen, und damit eine visuelle Überprüfung des Vorhandenseins der optischen Sicherheitsmerkmale durchgeführt worden ist. Des Weiteren kann eine Telefonaufzeichnung notwendig sein, um von Seiten der FMA überprüfen zu können, ob allenfalls vorliegende Unstimmigkeiten oder Unsicherheiten im Sinne des § 5 durch weitere Informationen ausgeräumt werden konnten oder ob der Vorgang der Online-Identifikation abzubrechen gewesen wäre.

Neben der durchgehenden akustischen Aufzeichnung der Online-Identifikation kommt der Aufzeichnung wesentlicher Momente der Identifikation durch Bildschirmkopien wesentliche Bedeutung zu. Kern der Identifizierung ist der Abgleich der Person mit dem vorgewiesenen amtlichen Lichtbildausweis und die Prüfung des letzteren. Deswegen muss einerseits das Gesicht der Person und andererseits der amtliche Lichtbildausweis von der Vorderseite, auf der das Lichtbild angebracht ist, und der Rückseite ebendieser Seite, der Datenseite, durch Bildschirmkopie dokumentiert werden. Dabei kann die Dokumentation ihren Zweck nur erfüllen, wenn geeignete Lichtverhältnisse herrschen, um die entsprechenden Überprüfungshandlungen setzen zu können. Das Gesicht kann jedenfalls mit dem Passbild abgeglichen werden. Wird die Online-Identifikation aber z. B. gemäß § 5 Z 2 abgebrochen, weil die Statur nicht zu den sonstigen Angaben im amtlichen Lichtbildausweis passt, bietet sich zu Dokumentationszwecken eine Bildschirmkopie von einem größeren Bildausschnitt an.

Um den Abgleich des Passbildes aus dem Lichtbildausweis mit dem tatsächlichen Gesicht des potentiellen Kunden oder seiner vertretungsberechtigten Person sicherzustellen und zu verhindern, dass dem Mitarbeiter zum Abgleich ein weiteres Foto präsentiert wird, soll der potentielle Kunde oder seine vertretungsberechtigte Person auf Aufforderung jedenfalls einmalig den Kopf bewegen und insofern die Illusion eines Standbildes vermieden werden. Um die Bildschirmkopie und die akustische Aufzeichnung miteinander zu verknüpfen, hat der potentielle Kunde oder dessen vertretungsbefugte natürliche Person während der Online-Identifikation die Seriennummer des amtlichen Lichtbildausweises mitzuteilen.

Mit der Verlesung der Seriennummer des Lichtbildausweises wird eine Verknüpfung zwischen den Bildschirmkopien des Lichtbildausweises und der Gesprächsaufzeichnung hergestellt und eine zusätzliche Sicherungsmaßnahme zur Verringerung des Risikos getroffen, dass der Kunde oder seine vertretungsberechtigte natürliche Person lediglich Bilder eines an dritter Stelle befindlichen Lichtbildausweises in die Bildübertragung einspielt.

Die Vergewisserung des Mitarbeiters des Verpflichteten oder des Dienstleisters über die Authentizität des vorgelegten amtlichen Lichtbildausweises hat durch mehrere, in der Verordnung klar bestimmte Prüfschritte zu erfolgen. Die optischen Sicherheitsmerkmale des Ausweises, die korrekte Ziffernorthographie und die Unversehrtheit der Laminierung des Ausweises sind zu überprüfen. Außerdem muss der Mitarbeiter überprüfen, ob keine Hinweise vorliegen, die darauf schließen lassen würden, dass das Lichtbild erst nachträglich mit dem amtlichen Lichtbildausweis verbunden worden ist. Schließlich ist die logische Konsistenz des amtlichen Lichtbildausweises selbst und im Verhältnis zum vorgegebenen Inhaber des Ausweises zu prüfen.

Abstrakte Beispiele für eine korrekte alphanumerische Ziffernorthographie der Seriennummer sehen für Österreich und Deutschland wie folgt aus:

Beispiel für den österreichischen Personalausweis:

Länge	Struktur
32	**1. Zeile:** **N** **Seriennummer** **PZ**
	I D A U T x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8 < p_{SN} < <<<<<<<<<<<<<<< <
	2. Zeile: **Geburtsdatum (invers)** **PZ** **G** **Ablaufdatum (invers)** **PZ** **N** **PZ**
	j j m m t t p_{GD} g j j m m t t p_{AD} A U T<<<<<<<<<<<<<p_{ges}
	3. Zeile: N a c h n a m e < < V o r n a me<<<<<<<<<<<<<< < <
N: Nationalität (AUT = Österreicher); G: Geschlecht (M oder F) p_{SN}: Prüfziffer der Seriennummer, p_{GD}: Prüfziffer des Geburtsdatums p_{AD}: Prüfziffer des Ablaufdatums, p_{ges}: Prüfziffer über alle Ziffern	

Beispiel für den österreichischen Reisepass:

Länge	Struktur
32	**1. Zeile:** N a c h n a m e < <Vorn a m e< < < <<<<<< < < <<
	2. Zeile: **Seriennummer** **PZ** **N** **Geburtsdatum (invers)** **PZ** **G** **Ablaufdatum (invers)** **PZ**
	a x_1 x_2 x_3 x_4 x_5 x_6 x_7 p_{SN} < AUT j j m m t t p_{GD} g j j m m t t p_{AD} < <<
a = A-Z; N = Nationalität (AUT = Österreicher); G = Geschlecht (M oder F) p_{SN}: Prüfziffer der Seriennummer, p_{GD}: Prüfziffer des Geburtsdatums p_{AD}: Prüfziffer des Ablaufdatums, p_{ges}: Prüfziffer über alle Ziffern	

Beispiel für den deutschen Personalausweis:

Länge	Struktur
36	**Seriennummer** (**Behörden-kennzahl** / **Fortlaufende Ausweisnummer**) **PZ** **N** **Geburtsdatum (invers)** **PZ** **Ablaufdatum (invers)** **PZ**
	x_1 x_2 x_3 x_4 y_1 y_2 y_3 y_4 y_5 p_{SN} D < < j j m m t t p_{GD} < j j m m t t p_{AD} <
N = Nationalität (D=Deutscher) p_{SN}: Prüfziffer der Seriennummer, p_{GD}: Prüfziffer des Geburtsdatums p_{AD}: Prüfziffer des Ablaufdatums, p_{ges}: Prüfziffer über alle Ziffern	

Beispiel für den deutschen Reisepass:

Länge	Struktur
44	**1. Zeile:** P < D < < N a c h n a me< < V o r n a me< < << < < <<<<<<<<<<<<<< < <
	2. Zeile: **Seriennummer** (**Behörden-kennzahl** / **Fortlaufende Ausweisnummer**) **PZ** **N** **Geburtsdatum (invers)** **PZ** **G** **Ablaufdatum (invers)** **PZ** **PZ**
	x_1 x_2 x_3 x_4 y_1 y_2 y_3 y_4 y_5 p_{SN} D < < j j m m t t p_{GD} g j j m m t t p_{AD} < <<<<<<<<<<<<<<p_{ges}
N = Nationalität (D = Deutscher); G = Geschlecht (M oder F) p_{SN}: Prüfziffer der Seriennummer, p_{GD}: Prüfziffer des Geburtsdatums p_{AD}: Prüfziffer des Ablaufdatums, p_{ges}: Prüfziffer über alle Ziffern	

Die mit einer Fernkommunikation einhergehenden Unsicherheiten sollen überdies durch Verwendung eines über E-Mail oder SMS funktionierenden TAN-Verfahrens ausgeglichen werden. Dazu ist während der Online-Identifikation eine währenddessen gültige Transaktionsnummer zentral zu generieren und an den potentiellen Kunden oder dessen vertretungsbefugte natürliche Person per E-Mail oder SMS, jedenfalls aber unabhängig vom Informationskanal der Online-Identifikation selbst zu übermitteln. Der potentielle Kunde oder dessen vertretungsbefugte natürliche Person hat die Transaktionsnummer sodann unmittelbar einzugeben und an den Mitarbeiter zurückzusenden.

Zu § 5:

Die Bestimmung berücksichtigt Fälle einer – faktisch oder zumindest in ihrer ursprünglichen Zielsetzung – gescheiterten Online-Identifikation.

Abs. 1 geht von dem Regelfall aus, dass aufgrund einer gescheiterten Online-Identifikation diese abzubrechen und keine Geschäftsbeziehung zu begründen ist. Ist eine visuelle Überprüfung des amtlichen Lichtbildausweises oder des potentiellen Kunden oder dessen vertretungsbefugter natürlicher Person oder von beiden nicht möglich, ist die Online-Identifikation jedenfalls abzubrechen. Eine derartige Unmöglichkeit kann sich zum Beispiel aufgrund schlechter Lichtverhältnisse, einer schlechten Bildqualität oder einer schlechten Bildübertragung ergeben. Störungen der sprachlichen Kommunikation werden im Übrigen regelmäßig zu sonstigen Unsicherheiten führen, die einen Abbruch rechtfertigen. Unstimmigkeiten führen jedenfalls dann zum Abbruch der Online-Identifikation, wenn sie nicht nachvollziehbar und zweifelsfrei aufgeklärt werden können.

Abs. 2 berücksichtigt Fälle, in denen Unsicherheiten oder Unstimmigkeiten einen der Fälle gemäß § 5 Z 4 oder 5 FM-GwG – oder auch beide Fälle – begründen und damit die ursprüngliche Zielsetzung der Online-Identifikation gescheitert ist. So können Unsicherheiten und Unstimmigkeiten den Verdacht oder den berechtigten Grund zur Annahme stützen, dass der Kunde einer terroristischen Vereinigung angehört oder objektiv an Transaktionen mitwirkt, die der Geldwäscherei (§ 165 des Strafgesetzbuches (StGB) – unter Einbeziehung von Vermögensbestandteilen, die aus einer strafbaren Handlung des Täters selbst herrühren) oder der Terrorismusfinanzierung dienen. Ebenso können sie Zweifel an der Echtheit der erhaltenen Kundenidentifikationsdaten hervorrufen. Diese Fälle verpflichten gemäß § 5 Z 4 und 5 in Verbindung mit § 6 Abs. 1 Z 1 FM-GwG zur Fortführung der Kundenidentifikation und können die weiteren Pflichten gemäß § 7 Abs. 7 FM-GwG nach sich ziehen, keine Geschäftsbeziehung zu begründen und eine Verdachtsmeldung gemäß § 16 FM-GwG an die Geldwäschemeldestelle zu erwägen. Abs. 2 betrifft damit anschaulich angesprochen folgende Vorgangsweise: Durchführung der Online-Identifikation – Verzicht auf die Begründung einer Kundenbeziehung – Verdachtsmeldung an die Geldwäschemeldestelle.

Zu § 6:

Die Bestimmung stellt klar, dass ein Dienstleister, dessen sich der Verpflichtete zum Zwecke der Durchführung der Online-Identifikation bedient, hinsichtlich des Umfanges und der Qualität gleichwertige Sicherungsmaßnahmen ergreifen muss, wie sie in dieser Verordnung festgelegt sind. Die endgültige Verantwortung für die Einhaltung der Anforderungen verbleibt jedoch bei dem sich eines Dienstleisters bedienenden Verpflichteten. Korrespondierend dazu, dass der Dienstleister Pflichten des Verpflichteten erfüllt, treffen den letzteren besondere Sorgfaltspflichten bei Abschluss, Durchführung und allfälliger Kündigung der Vereinbarung mit dem Dienstleister. Dabei ist auf eine klare, ausdrückliche und schriftlich festgehaltene Aufteilung der Rechte und Pflichten zu achten.

Auslagerungs- und Vertretungsverhältnisse im Sinne von § 15 FM-GwG dürfen weder interne Kontrollen einschließlich solcher durch den Abschlussprüfer noch solche durch die FMA beeinträchtigen.

Zu § 7:

Die Bestimmung regelt Verweise auf bundesgesetzliche Bestimmungen.