

Entwurf

Verordnung der Finanzmarktaufsichtsbehörde (FMA), mit der die Online-Identifikationsverordnung geändert wird

Auf Grund des § 6 Abs. 4 des Finanzmarkt-Geldwäschegesetzes – FM-GwG, BGBl. I Nr. 118/2016, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 25/2021, wird mit Zustimmung des Bundesministers für Finanzen verordnet:

Die Online-Identifikationsverordnung (Online-IDV), BGBl. II Nr. 5/2017, zuletzt geändert durch die Verordnung BGBl. II Nr. 414/2020, wird wie folgt geändert:

1. Am Ende des § 2 Z 3 wird der Punkt durch einen Strichpunkt ersetzt und folgende Z 4 angefügt:

„4. Biometrische Identifikationsverfahren: Verfahren zur Online-Identifikation, bei denen die gesamte Online-Identifikation oder einzelne Schritte davon ohne Beteiligung eines Mitarbeiters im Rahmen eines automatisierten elektronischen Verfahrens durchgeführt werden.“

2. § 4 Abs. 3 Z 2 lautet:

„2. die Seriennummer seines amtlichen Lichtbildausweises oder eine vom Verpflichteten zufällig generierte, mindestens acht Zeichen umfassende Zeichen- oder Wortfolge mitzuteilen.“

3. Dem § 4 wird folgender Abs. 6 angefügt:

„(6) Die Online-Identifikation kann auch durch geeignete Biometrische Identifikationsverfahren erfolgen. Dabei sind die Anforderungen dieser Verordnung nach Maßgabe der folgenden Bestimmungen einzuhalten:

1. Das Biometrische Identifikationsverfahren muss jedenfalls dem aktuellen Stand der Technik entsprechen, anlassbezogen aktualisiert werden und ein Sicherheitsniveau erreichen, mit dem zumindest eine der Online-Identifikation durch Mitarbeiter gleichwertige Erfüllung sichergestellt werden kann. Der Verpflichtete muss geeignete Maßnahmen zur Sicherung der Integrität und Sicherheit der verwendeten Verfahren treffen, einschließlich aktiver Überwachungsmaßnahmen, um etwaige Probleme unmittelbar zu erkennen und zu beseitigen.
2. Das Biometrische Identifikationsverfahren ist vom Verpflichteten nachvollziehbar zu dokumentieren. Abs. 2 erster Satz ist mit der Maßgabe anzuwenden, dass Aufnahmen, die zum Zwecke der Online-Identifikation erstellt werden, in ihrer Gesamtheit vom Verpflichteten akustisch und optisch aufzuzeichnen sind. Die Dokumentation umfasst jedenfalls auch die im Rahmen der Überprüfung herangezogenen Sicherheitsfaktoren und die Ergebnisse der einzelnen Prüfungsschritte.
3. Abs. 2 Z 2 und 3 ist mit der Maßgabe anzuwenden, dass anstelle der Anfertigung von Bildschirmkopien bei der Überprüfung elektronisch signierter Lichtbildausweise (Z 5) die elektronisch signierten Daten zu speichern sind.
4. Werden die Anforderungen gemäß Abs. 3 und 5 durch ein Biometrisches Identifikationsverfahren erfüllt, überprüft der Verpflichtete die tatsächliche Teilnahme des potentiellen Kunden oder seiner vertretungsbefugten natürlichen Person an der Online-Identifikation anhand geeigneter Sicherungsmaßnahmen, die jedenfalls die Überprüfung anhand einer während der Online-Identifikation erstellten Videoaufnahme umfassen (Liveness-Check). Der Liveness-Check kann von Abs. 3 Z 1 und 2 und Abs. 5 abweichen und ist vom Verpflichteten akustisch und optisch aufzuzeichnen und aufzubewahren.

5. Für Biometrische Identifikationsverfahren dürfen nur Lichtbildausweise, deren Inhalt von der ausstellenden Behörde elektronisch signiert worden ist, verwendet werden. Der Verpflichtete hat dabei die Echtheit der elektronischen Signatur des Lichtbildausweises und die Integrität der elektronisch signierten Daten zu überprüfen und sicherzustellen, dass zur Signatur kein kompromittierter Schlüssel verwendet worden ist. Im Rahmen des Biometrischen Identifikationsverfahrens hat der Verpflichtete auch eine Überprüfung der logischen Konsistenz gemäß Abs. 4 Z 5 vorzunehmen. Abs. 4 Z 1 bis 4 ist auf die Überprüfung der Authentizität des Lichtbildausweises im Rahmen eines Biometrischen Identifikationsverfahrens nicht anwendbar.“

4. § 5 Abs. 1 Z 1 lautet:

„1. eine geeignete Überprüfung des potentiellen Kunden oder des amtlichen Lichtbildausweises oder von beiden unter Berücksichtigung der verfahrensbezogenen Sicherungsmaßnahmen (§ 4) nicht möglich ist,“

5. In § 9 wird das Datum „30. Juni 2021“ durch „31. Dezember 2021“ ersetzt.

6. Der bisherige § 9 erhält die Absatzbezeichnung „(1)“ und es wird folgender Abs. 2 angefügt:

„(2) § 2 Z 3 und 4, § 4 Abs. 3 Z 2 und Abs. 6 sowie § 5 Abs. 1 Z 1 in der Fassung der Verordnung BGBl. II Nr. XXX/2021 treten mit 1. Juli 2021 in Kraft. Zwischen 1. Juli 2021 und 31. März 2022 können Verpflichtete abweichend von § 4 Abs. 6 Z 5 in der Fassung der Verordnung BGBl. II Nr. XXX/2021 Biometrische Identifikationsverfahren ohne Überprüfung der elektronischen Signatur des Lichtbildausweises einsetzen, sofern das Verfahren § 4 Abs. 4 Z 1 bis 5 entspricht.“

Begründung

Allgemeiner Teil

§ 6 Abs. 4 Z 1 des Finanzmarkt-Geldwäschegesetzes (FM-GwG), BGBl. I Nr. 118/2016, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 25/2021, erlaubt die Überprüfung der Identität eines Kunden durch Vorlage des amtlichen Lichtbildausweises im Rahmen eines videogestützten elektronischen Verfahrens (Online-Identifikation). In der Online-Identifikationsverordnung (Online-IDV), BGBl. II Nr. 5/2017, zuletzt geändert durch die Verordnung BGBl. II Nr. 414/2020, werden gemäß § 6 Abs. 4 letzter Satz FM-GwG die Maßnahmen festgelegt, die bei der Online-Identifikation vom Verpflichteten zum Ausgleich des erhöhten Risikos aufgrund der fehlenden persönlichen Anwesenheit des Kunden einzuhalten sind.

Mit der vorliegenden Novelle der Online-IDV werden die Anforderungen an die Online-Identifikation im Rahmen eines Biometrischen Identifikationsverfahrens festgelegt. Aufgrund des technischen Fortschrittes sind mittlerweile neue Verfahren verfügbar, die nicht mehr auf natürliche Personen für die Durchführung der Online-Identifikation zurückgreifen, sondern auf künstlicher Intelligenz basierende elektronische Videosysteme verwenden. Diese sog. Biometrischen Identifikationsverfahren sollen als eine zusätzliche Möglichkeit der Fernidentifizierung vorgesehen werden. Voraussetzung ist, dass das Biometrische Identifikationsverfahren die in der Online-IDV vorgesehenen Anforderungen erfüllt. Dazu zählen insbesondere die organisatorischen (§ 3) und verfahrensbezogenen (§ 4) Sicherungsmaßnahmen, wobei in § 4 Abs. 6 spezifische Anforderungen an Biometrische Identifikationsverfahren vorgesehen werden.

Besonderer Teil

Zu Z 1 (§ 2 Z 4):

Definiert den Begriff „Biometrisches Identifikationsverfahren“. Biometrische Identifikationsverfahren können, soweit sie den gesetzlichen Anforderungen entsprechen (dazu zählt neben § 4 insbesondere auch § 3 Abs. 2), zur Erfüllung einzelner oder aller in § 4 genannten verfahrensbezogenen Sicherungsmaßnahmen eingesetzt werden.

Zu Z 2 (§ 4 Abs. 3 Z 2):

Auch bei der gewöhnlichen Online-Identifikation durch einen Mitarbeiter des Verpflichteten ist es künftig möglich, dass der Kunde anstelle der Seriennummer seines Lichtbildausweises eine vom Verpflichteten zufällig generierte, zumindest achtstellige Zeichen- oder Wortfolge vorliest. Damit werden die Anforderungen an die Online-Identifikation an die Anforderungen an den Liveness-Check im Rahmen einer Biometrischen Identifikation angenähert (Abs. 6 Z 4). Als Zeichenfolge gilt auch eine Ziffernfolge.

Zu Z 3 (§ 4 Abs. 6):

Abs. 6 regelt die Anforderungen an Biometrische Identifikationsverfahren, die bei der Online-Identifikation Einsatz finden. Biometrische Identifikationsverfahren konnten schon bisher zur Unterstützung des die Online-Identifikation durchführenden Mitarbeiters des Verpflichteten eingesetzt werden (etwa durch Warnungen, wenn ein algorithmisches System Auffälligkeiten feststellt). Zukünftig erlaubt Abs. 6, dass geeignete Biometrische Identifikationsverfahren die Durchführung der Online-Identifikation durch einen Mitarbeiter auch ersetzen können. Es können dabei einzelne oder alle der unter den Abs. 1 bis 5 festgelegten verfahrensbezogenen Sicherungsmaßnahmen durch ein Biometrisches Identifikationsverfahren erfüllt werden. Zulässig sind daher auch Verfahren, bei denen die Online-Identifikation grundsätzlich weiterhin durch einen Mitarbeiter erfolgt, aber einzelne Überprüfungsschritte (etwa die Überprüfung der Echtheit des Lichtbildausweises anhand der elektronischen Ausweissignatur) automationsunterstützt durchgeführt werden. Der Mitarbeiter muss in letzterem Fall den Überblick über die gesamte Online-Identifikation einschließlich der biometrisch durchgeführten Sicherungsmaßnahmen haben, um etwa Inkonsistenzen zwischen den einzelnen Überprüfungsschritten erkennen und angemessen berücksichtigen zu können.

Voraussetzung für den Einsatz von Biometrischen Identifikationsverfahren ist, dass das Verfahren allen gesetzlichen Anforderungen an die Online-Identifikation entspricht und eine ordnungsgemäße Feststellung und Überprüfung der Identität einer Person erlaubt. Zu den einzuhaltenden Anforderungen zählen insbesondere auch die EDV-bezogenen organisatorischen Sicherungsmaßnahmen gemäß § 3 Abs. 2 und die verfahrensbezogenen Sicherungsmaßnahmen gemäß § 4 Abs. 1 bis 5. Darüber hinaus sieht Abs. 6 eigene Anforderungen an Biometrische Identifikationsverfahren vor, die die verfahrensbezogenen Sicherungsmaßnahmen des § 4 Abs. 1 bis 5 anpassen. Sonstige Anforderungen in der Online-IDV an die Mitarbeiter, die die Online-Identifikation durchführen, (siehe § 3 Abs. 1, 3 und 4 zur Schulung von

Mitarbeitern und zu den Räumen, in denen die Online-Identifikation vom Mitarbeiter durchgeführt wird) sind bei Biometrischen Identifikationsverfahren dagegen ohne Anwendungsbereich, soweit das Verfahren ohne direkte Beteiligung von Mitarbeitern erfolgt. Für die notwendige Verfahrenssicherheit sind stattdessen insbesondere § 3 Abs. 2 und § 4 Abs. 6 Z 1 einschlägig.

Ist eine Biometrische Identifikation mit hinreichender Sicherheit nicht möglich, so ist die Online-Identifikation gemäß § 5 abubrechen. Verpflichtete können auch vorsehen, dass in Zweifelsfällen die Online-Identifikation durch einen Mitarbeiter des Verpflichteten fortgesetzt wird, wenn durch den Mitarbeiter die Zweifel ausgeräumt werden können.

Zu Z 1: Z 1 enthält allgemeine Anforderungen, die von allen Biometrischen Identifikationsverfahren erfüllt werden müssen. Vom Verpflichteten ist in regelmäßigen Abständen zu evaluieren, ob das angewendete Biometrische Identifikationsverfahren noch dem aktuellen Stand der Technik entspricht. Dabei sind insbesondere auch Informationen und Warnhinweise von verlässlichen nationalen und internationalen Quellen zu (Biometrischen) Identifikationsverfahren zu berücksichtigen. Das Ergebnis und allfällige weitere Schritte sind zu dokumentieren.

Zu Z 2: Sowohl das eingesetzte Verfahren selbst, einschließlich der Einhaltung der Anforderungen gemäß Z 1, als auch die durchgeführten Biometrischen Identifikationen sind nachvollziehbar zu dokumentieren. Die Dauer der Aufbewahrung richtet sich nach § 21 FM-GwG. Die Dokumentation umfasst jedenfalls auch die im Rahmen der Überprüfung herangezogenen Sicherheitsfaktoren und die Ergebnisse der einzelnen Prüfungsschritte. Dabei handelt es sich um die „Scoring“-Werte, die im Rahmen solcher Verfahren für die einzelnen Sicherheitsfaktoren berechnet werden. Es geht dabei nicht nur um die Ergebnisse selbst, sondern auch um die Zusammensetzung des jeweiligen Ergebnisses und die Beschreibung der Sicherheitsfaktoren, die in dem jeweiligen Verfahren herangezogen werden.

Zu Z 3: Bei einer Speicherung der elektronisch signierten Ausweisdaten ist eine darüberhinausgehende Anfertigung von Ausweiskopien grundsätzlich nicht erforderlich.

Zu Z 4: Zentraler Bestandteil der Online-Identifikation ist neben der Überprüfung des Lichtbildausweises die Verifizierung, dass die im Ausweis beschriebene Person auch tatsächlich an der Online-Identifikation teilnimmt. Im Rahmen Biometrischer Identifikationsverfahren ist dafür der Begriff „Liveness-Check“ gebräuchlich. Beim Liveness-Check ist sicherzustellen, dass auch tatsächlich eine Person am Endgerät des Kunden an der Online-Identifikation teilnimmt (und nicht etwa historische Aufnahmen abgespielt werden oder die tatsächliche Präsenz einer Person durch algorithmisch generierte Aufnahmen simuliert wird) und dass es sich bei der teilnehmenden Person auch tatsächlich um die im Lichtbildausweis bezeichnete Person handelt. Der Liveness-Check muss diese Überprüfung jedenfalls anhand einer während der Online-Identifikation herzustellenden Videoaufnahme durchführen, zumal es sich bei der Online-Identifikation gemäß § 6 Abs. 4 Z 1 FM-GwG notwendigerweise um ein videogestütztes Verfahren handelt. Wie diese Videoaufnahme konkret ausgestaltet wird und welche weiteren Sicherungsmaßnahmen vorgesehen werden, wird von der Online-IDV im Sinne der Technologieneutralität nicht vorgegeben. Solche Liveness-Checks können etwa darin bestehen, dass die zu identifizierende Person eine vom Verpflichteten vorgegebene Zeichen- oder Wortfolge vorzulesen hat, mehrmalig einen vom Verpflichteten zufällig auf dem Bildschirm ausgewählten Bereiche mittels Kopfbewegungen nachzuverfolgen hat oder nach einer Aufforderung den Kopf in unterschiedliche Richtungen zu bewegen hat. Jedenfalls muss der Liveness-Check den allgemeinen Anforderungen entsprechen, also insb. gemäß Z 1 dem aktuellen Stand der Technik entsprechen und eine sichere Identifikation erlauben. In Zweifelsfällen ist die Online-Identifikation abubrechen (§ 5) oder durch einen Mitarbeiter des Verpflichteten fortzusetzen.

Zu Z 5: Biometrische Identifikationsverfahren müssen die Echtheit des Lichtbildausweises ab 1. April 2022 (§ 9 Abs. 2) anhand der elektronischen Ausweissignatur überprüfen. Zur Überprüfung durch ein Auslesen der elektronisch gespeicherten Daten kommen insbesondere Reisepässe in Frage. Spätestens seit 2007 ist die Ausstellung biometrischer Reisepässe mit NFC-Chip international Standard. Auch die Verbreitung von NFC-fähigen Mobiltelefonen hat mittlerweile ein hohes Niveau erreicht. Daher bestehen keine hinreichenden Gründe mehr, um bei der biometrischen Identifikation neben der besonders fälschungssicheren Überprüfung anhand der elektronisch gespeicherten Daten auch eine weniger fälschungssichere, rein optische Überprüfung des Lichtbildausweises anhand einer vom Nutzer erstellten Bildaufnahme zuzulassen. Weiterhin zulässig bleibt die Überprüfung des Lichtbildausweises durch einen Mitarbeiter ohne Prüfung der elektronischen Signatur gemäß § 4 Abs. 4.

Verpflichtete haben bei der Prüfung der elektronischen Signatur durch Einsicht in geeignete Datenbanken sicherzustellen, dass zur Signatur kein kompromittierter Schlüssel verwendet worden ist, der unbefugten Dritten die Erstellung gefälschter Signaturen erlauben würde. Einschlägige Datenbanken werden etwa von der Internationalen Zivilluftfahrtorganisation (ICAO) unterhalten (<https://download.pkd.icao.int/>). Von

einer Kompromittierung ist insbesondere auszugehen, wenn unbefugte Dritte Kenntnis vom zur Signatur verwendeten privaten Schlüssel erlangt haben.

Zu Z 4 (§ 5 Abs. 1 Z 1):

Z 1 wird sprachlich an den neuen § 4 Abs. 6 über Biometrische Identifikationsverfahren angepasst.

Zu Z 5 und 6 (§ 9):

Inkrafttretensbestimmung. Die zeitlich befristete Regelung des § 3 Abs. 4, die eine Online-Identifikation durch Mitarbeiter im Home-Office ermöglicht, wird bis 31. Dezember 2021 verlängert, da die COVID 19-Pandemie weiterhin andauert.

Die Regelungen zur biometrischen Identifikation treten mit 1. Juli 2021 in Kraft. Bis 31. März 2022 können dabei auch Biometrische Identifikationsverfahren eingesetzt werden, die die Echtheit des Lichtbildausweises lediglich optisch überprüfen. Diesfalls ist auch eine Bildaufnahme des Lichtbildausweises zu speichern (§ 4 Abs. 2 in Verbindung mit Abs. 6 Z 3).