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. 98/2021, 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. 265/2021, 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 3):

Verweisaktualisierung

Zu Z 2 (§ 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 3 (§ 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 vierstellige Zeichen- oder Wortfolge vorliest. Als Zeichenfolge gilt auch eine Ziffernfolge.

Zu Z 4 (§ 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, siehe zu den datenschutzrechtlichen Anforderungen sogleich). 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.

Die Bestimmungen über den Einsatz Biometrischer Identifikationsverfahren gemäß Abs. 6 gelten unbeschadet der anwendbaren datenschutzrechtlichen Anforderungen (siehe § 1 Abs. 4). Wie im Einleitungssatz des Abs. 6 klargestellt wird, stellt die Online-IDV insbesondere auch keine Bestimmung im Sinne des Art. 9 Abs. 2 Buchstabe g der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119 vom 04.05.2016 S. 1, in der Fassung der

Berichtigung ABl. Nr. L 74 vom 04.03.2021 S. 35, dar. Die Online-Identifikation im Rahmen eines Biometrischen Identifikationsverfahrens gemäß Abs. 6 stellt eine Verarbeitung personenbezogener biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person dar, die gemäß Art. 9 Abs. 1 der Verordnung (EU) 2016/679 grundsätzlich untersagt ist. Eindeutige biometrische Identifikationen sind gemäß Art. 9 Abs. 2 der Verordnung (EU) 2016/679 daher nur erlaubt, wenn einer der dort aufgezählten, taxativen Ausnahmetatbestände erfüllt ist. Erlaubt wäre etwa gemäß Buchstabe g des Art. 9 Abs. 2 der Verordnung (EU) 2016/679 eine Verarbeitung, die auf der Grundlage des Rechts eines Mitgliedstaats aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist. Die Online-IDV erfordert eine biometrische Personenidentifizierung aber gerade nicht, sondern es steht dem Verpflichteten frei, die Identität des Kunden durch eigene Mitarbeiter zu überprüfen, ohne dass es zu einer Verarbeitung biometrischer Daten im Sinne des Art. 9 Abs. 1 der Verordnung (EU) 2016/679 kommt. Voraussetzung für die Identifikation eines Kunden im Rahmen eines Biometrischen Identifikationsverfahrens im Sinne des Abs. 6 ist daher, dass die betroffene Person gemäß Art. 9 Abs. 2 Buchstabe a der Verordnung (EU) 2016/679 wirksam in die biometrische Verarbeitung eingewilligt hat. Bei der Einholung der Einwilligung des Kunden ist Art. 7 der Verordnung (EU) 2016/679 zu beachten. Insbesondere muss die Einwilligung gemäß Art. 7 Abs. 4 der Verordnung (EU) 2016/679 freiwillig erfolgen. Eine freiwillige Einwilligung liegt nur vor, wenn der Betroffene eine echte und freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden (vergleiche Erwägungsgrund 42 der Verordnung (EU) 2016/679). Für die Freiwilligkeit der Zustimmung spricht es daher etwa, wenn Betroffenen als Alternative zur Biometrischen Identifikation eine Online-Identifikation durch Mitarbeiter des Verpflichteten angeboten wird. Jedenfalls sollten Kunden in diesem Zusammenhang darauf hingewiesen werden, dass alternative Identifikationsmöglichkeiten bestehen.

Zu den weiteren datenschutzrechtlichen Anforderungen, die vom Verpflichteten im Zusammenhang mit Abs. 6 zu beachten sind, zählen insbesondere die Anforderungen an die Aufbewahrung personenbezogener Daten gemäß § 21 FM-GwG, die Datensicherheitsmaßnahmen gemäß Art. 32 der Verordnung (EU) 2016/679 und die Bestimmungen zur Durchführung von Datenschutz-Folgenabschätzungen gemäß Art. 35 der Verordnung (EU) 2016/679, § 21 Abs. 2 des Datenschutzgesetzes (DSG), BGBl. I Nr. 165/1999, und § 2 Abs. 2 Z 4 der Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V), BGBl. II Nr. 278/2018. Aufgrund ihrer besonderen Wichtigkeit wird im Einleitungssatz des Abs. 6 ausdrücklich klargestellt, dass die Zulässigkeit biometrischer Identifikationsverfahren im Rahmen der Online-IDV unter dem Vorbehalt angemessener Sicherheitsmaßnahmen im Sinne des Art. 32 der Verordnung (EU) 2016/679 steht. Anwendbar können auch die Bestimmungen des Art. 22 der Verordnung (EU) 2016/679 sein, wonach betroffene Personen (vorbehaltlich der dort in den Abs. 2 ff genannten Einschränkungen) das Recht haben, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihnen gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Relevant wäre es in dem Zusammenhang insbesondere, wenn ein Verpflichteter ausschließlich aufgrund einer fehlgeschlagenen biometrischen Identifikation einen Vertragsabschluss ablehnt, ohne etwa den Identifikationsversuch mit einem Mitarbeiter fortzusetzen (vgl. *Buchner* in *Kühling/Buchner*, DS-GVO, Art. 22 Rz 15 f). Liegt eine automatisierte Entscheidung im Einzelfall vor, ist insbesondere auch Art. 22 Abs. 2 bis 4 der Verordnung (EU) 2016/679 zu beachten. Die Online-IDV stellt dabei auch keine Öffnungsklausel im Sinne des Art. 22 Abs. 2 Buchstabe b der Verordnung (EU) 2016/679 dar. Daher hat der Verantwortliche, soweit eine automatisierte Entscheidung im Sinne des Art. 22 der Verordnung (EU) 2016/679 vorliegt, gemäß dessen Abs. 3 angemessene Maßnahmen zu treffen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren (siehe insoweit auch Abs. 4 desselben Artikels), wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört. Wird dementsprechend ein Identifikationsversuch durch Mitarbeiter des Verpflichteten überprüft oder fortgesetzt, so sind dabei auch die einschlägigen Anforderungen der Online-IDV und des FM-GwG an die Feststellung und Überprüfung der Identität des Kunden durch Mitarbeiter des Verpflichteten zu beachten.

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 § 4 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 abzubrechen. 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 § 4 Abs. 6 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. Zudem ist eine laufende technische Überwachung des eingesetzten Verfahrens erforderlich, um etwaige auftretende Probleme unmittelbar erkennen und beseitigen zu können. Bedient sich der Verpflichtete eines Auftragsverarbeiters gemäß § 6, wird es dabei in der Regel zielführend sein, dass auch der Auftragsverarbeiter diese Überwachung durchführt. Dabei ist es aber nicht erforderlich, jede einzelne Kundenidentifizierung durch Mitarbeiter überprüfen zu lassen, soweit eine sichere Kundenidentifizierung durch technische Maßnahmen sichergestellt ist.

Die in dieser Verordnung vorgesehenen verfahrensbezogenen Anforderungen stellen Mindestanforderungen dar, die bei jeder einzelnen Online-Identifikation im Rahmen eines Biometrischen Identifikationsverfahrens anzuwenden sind. Selbstverständlich können Verpflichtete darüber hinaus zusätzliche verfahrensbezogene Maßnahmen anwenden. Verpflichtete sollten deshalb im Rahmen eines risikobasierten Ansatzes auch regelmäßig überprüfen, ob unter Berücksichtigung der Risiken des verwendeten technischen Verfahrens generell oder in bestimmten Fällen weitere Sicherheitsmaßnahmen eingesetzt werden sollten, um eine ausreichende Verfahrenssicherheit zu gewährleisten. Zusätzlich könnten beispielsweise optische Überprüfungen der Sicherheitsmerkmale des Lichtbildausweises, Referenzüberweisungen, Adressverifizierungen, der Login im Kundenkonto bei einem anderen Institut im Wege eines Kontoinformationsdienstleisters oder eine Verifizierung der Daten beim Mobilfunkanbieter des Kunden für eine verbesserte Sicherheit sorgen. Auch die in § 4 Abs. 5 für die Online-Identifikation durch Mitarbeiter verpflichtend vorgesehene Überprüfung anhand eines Einmal-Codes kann im Rahmen eines Biometrischen Identifikationsverfahrens optional als zusätzliche Maßnahme zum Einsatz kommen. Letztlich entscheidend ist, dass das verwendete Verfahren jedenfalls die vorgeschriebenen sicherheitsbezogenen Mindestanforderungen der Online-IDV implementiert, und in Verbindung mit etwaigen zusätzlichen, vom Verpflichteten verwendeten Sicherungsmaßnahmen eine hinreichend sichere Feststellung und Überprüfung der Identität des Kunden erlaubt.

Zu § 4 Abs. 6 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 und der Umfang der aufzubewahrenden Informationen richtet sich grundsätzlich nach § 21 Abs. 1 Z 1 FM-GwG. Da sich die Verpflichtung zur Aufbewahrung unmittelbar aus dem Gesetz ergibt, ist sie auch von der Zustimmung der betroffenen Person unabhängig. 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. Aufnahmen, die zum Zwecke der biometrischen Identifikation erstellt worden sind, sind in der Form, in der sie erstellt worden sind, als elektronische Mittel im Sinne des § 21 Abs. 1 Z 1 FM-GwG aufzubewahren. Es kann sich dabei etwa um Videoaufnahmen mit oder ohne Ton, reine Tonaufnahmen oder Fotos handeln.

Zu § 4 Abs. 6 Z 3: Bei einer Speicherung der elektronisch signierten Ausweisdaten ist eine darüberhinausgehende Anfertigung von Ausweiskopien grundsätzlich nicht erforderlich, soweit alle relevanten Ausweisdaten auch elektronisch gespeichert worden sind.

Zu § 4 Abs. 6 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. Dies wird in der Online-IDV als Anwesenheitsprüfung bezeichnet, und entspricht dem bei Biometrischen Identifikationsverfahren verbreiteten Begriff des „Liveness-Checks". Bei der Anwesenheitsprüfung 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. Diese Überprüfung muss jedenfalls anhand einer während der Online-Identifikation herzustellenden Videoaufnahme durchgeführt werden, zumal es sich bei der Online-Identifikation gemäß § 6 Abs. 4 Z 1 FM-GwG notwendigerweise um ein videogestütztes Verfahren handelt. Nicht zwingend erforderlich ist dabei aber eine akustische Überprüfung. Grundsätzlich möglich ist es auch, die erforderliche Videoaufnahme mithilfe der Fotofunktion des Mobiltelefons des Kunden zu erstellen, welche womöglich qualitativ bessere Aufnahmen erlaubt als die Videofunktion. Entscheidend ist dabei, dass die erstellten Einzelbilder zeitlich so eng aufeinanderfolgen, dass sie gemeinsam eine Videoaufnahme im Sinne der Aufnahme eines Bewegtbildes darstellen. Selbstverständlich ist es auch möglich, einzelne Fotos ergänzend zur Erstellung einer Videoaufnahme aufzunehmen. Die zur Anwesenheitsprüfung erstellten Aufnahmen sind gemäß Z 2 in Verbindung mit § 21 Abs. 1 Z 1 FM-GwG aufzubewahren.

Wie diese Videoaufnahme konkret ausgestaltet wird und welche weiteren Sicherungsmaßnahmen vorgesehen werden, wird von der Online-IDV im Sinne der Technologieneutralität nicht vorgegeben. Solche Anwesenheitsprüfungen 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 Bereich mittels Kopfbewegungen nachzuverfolgen hat oder nach einer Aufforderung den Kopf in unterschiedliche Richtungen zu bewegen hat. Auch passive Prüfungen ohne Aufforderung an den Kunden zur Setzung eines bestimmten Verhaltens sind bei entsprechender technischer Eignung zulässig. Jedenfalls muss die Anwesenheitsprüfung 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 abzubrechen (§ 5) oder durch einen Mitarbeiter des Verpflichteten fortzusetzen.

Zu § 4 Abs. 6 Z 5: Biometrische Identifikationsverfahren müssen die Echtheit des Lichtbildausweises ab 1. Jänner 2023 (§ 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. Der Verpflichtete kann lediglich ergänzend zur Überprüfung anhand der elektronischen Signatur eine optische Ausweisprüfung durchführen. 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 5 (§ 5 Abs. 1 Z 1):

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

Zu Z 6 (§ 9):

Die Regelungen zur biometrischen Identifikation treten mit dem auf die Kundmachung folgenden Tag in Kraft. Bis 31. Dezember 2022 können dabei auch Biometrische Identifikationsverfahren eingesetzt werden, die die Echtheit des Lichtbildausweises lediglich optisch überprüfen. In diesem Rahmen können auch Lichtbildausweise zur Identifikation verwendet werden, die nicht elektronisch signiert sind. Diesfalls ist auch eine Bildaufnahme des Lichtbildausweises zu speichern (§ 4 Abs. 2 in Verbindung mit § 4 Abs. 6 Z 3).