WIRTSCHAFTSKAMMER ÖSTERREICH
Die Finanzdienstleister

Österreichische Finanzmarktaufischt
Otto-Wagner-Platz 5
1090 Wien

e-mail: begutachtung@fma.gv.at

Fachverband Finanzdienstleister
Bundessparte Information und Consulting
Wirtschaftskammer Österreich
Wiedner Hauptstraße 63 | 1045 Wien
T 05 90 900-4818| F 05 90 900-4817
E finanzdienstleister@wko.at
W https://wko.at/finanzdienstleister

Datum
09.04.2020

Stellungnahme zur Begutachtung einer Verordnung zur Änderung der Online-Identifikationsverordnung BGBl. II Nr. 199/2018 der FMA

Der Fachverband Finanzdienstleister bedankt sich für die Möglichkeit zum oben genannten Entwurf Stellung nehmen zu können und darf folgende Anmerkungen übermitteln:

Mit diesem Schreiben möchten wir zur Verordnung der Finanzmarktaufsichtsbehörde („FMA"), mit der die Online-Identifikationsverordnung idF BGBl. II Nr. 199/2018 („Online-IDV") geändert wird, wie folgt Stellung nehmen.

1. Übergangsbestimmung § 7a Online-IDV
1.1. Temporäre Beschränkung

Die vor dem Hintergrund der gegenwärtigen Situation mit der COVID-19 Pandemie vorgeschlagene temporäre Änderung der Online-IDV durch die Übergangsbestimmung § 7a sehen wir grundsätzlich positiv. Die Änderung sollte aus unserer Perspektive allerdings nicht zeitlich befristet werden, da diese unseres Erachtens **allgemein sinnvoll** sind. Viele Anbieter von Video-Identifizierungen arbeiten mit Cloudlösungen oder eigenen zentralen Servern auf die ihre Mitarbeiter mittels den vom Anbieter zur Verfügung gestellten Laptops über eine sichere Verbindung (zB VPN) zugreifen, um die Identifikationsdienstleistung zu erbringen. Da Anbieter in diesem Bereich meist versuchen ihre Leistungen nach einem besonders hohen Standard im Bereich IT und Datensicherheit anzubieten und dementsprechend auch Richtlinien sowie Compliance-Maßnahmen existieren, kann zumindest auch angenommen werden, dass diese auch beim Übergang in das Homeoffice weiter zur Anwendung kommen. Zudem müssen Mitarbeiter, die im Bereich Online-Identifikation zum Einsatz kommen, ohnedies entsprechend auf ihre Tätigkeit geschult und auf ihre Zuverlässigkeit geprüft werden, wobei gemäß § 3 Abs. 1 Online-IDV über den rechtlichen Rahmen, die technischen Voraussetzungen sowie die praktische Sicherstellung informiert werden muss. Im Sinne eines digitalen und dezentralen Ansatzes sowie flexibler Arbeitszeitmodelle, wäre somit die generelle Änderung der Online-IDV im Sinne des § 7a ohne temporäre Beschränkung gegebenenfalls unter der Vorgabe weiterer Sicherungsmaßnahmen zu begrüßen.

1.2. Alternative Identifikationsmöglichkeiten

Der Teil des vorletzten Satzes in § 7a Online-IDV „…und auf alternative Identifikationsmöglichkeiten hinzuweisen." ist unseres Erachtens unpraktikabel. In den meisten Fällen wird der Service von Identifikationsanbietern über eine Schnittstelle (API) in das System des jeweiligen regulierten Instituts eingebunden, was zur Folge hat, dass der Kunde beim Nutzung des Dienstes einerseits schon mehrere Anbieter zur Verfügung hat (auch entsprechend der Verpflichtungen zur Auslagerung der FMA) und nach der Weiterleitung an den Identifikationsanbietern sich bei einem vom regulierten Institut externen Provider befindet. Um den gegenständlichen Hinweis auf alternative Identifikationsmöglichkeiten zu

erfüllen, müsste der entsprechende Provider dann in vielen Fällen auf ein zu ihm in Konkurrenz stehendes Unternehmen verweisen und zudem kann der Mitarbeiter den Kunden aufgrund der technischen Gegebenheiten auch nicht direkt an den anderen Identifikationsanbietern weiterverweisen. Des Weiteren bräuchte der Identifikationsanbieter dann mehrere Workflows, je nachdem ob sich ein Mitarbeiter im Homeoffice befindet oder nicht, wobei der Workflow wiederrum aufgrund der Pflicht zur alternativen Identifikationsmöglichkeiten auch noch mit dem jeweiligen regulierten Institut abzustimmen wäre. Erhält der Kunde durch den Mitarbeiter die Information, dass sich dieser im Homeoffice befindet, kann der Kunde ohnedies den Vorgang selbstständig abbrechen und kommt zurück auf die Seite des regulierten Instituts und kann hierbei eine andere Form der Identifikation auswählen (sofern überhaupt verfügbar – diese Entscheidung wird wohl in der Privatautonomie der Unternehmen verbleiben müssen). Allerdings ist die Notwendigkeit des Hinweises an den Kunden auf die Tatsache, dass sich der durchführende Mitarbeiter gerade im Homeoffice befindet, unter Anbetracht der strengen Sicherheitsvorgaben ebenso zu hinterfragen und erscheint unseres Erachtens nicht geboten.

2. Änderung der Online-IDV im Hinblick auf automationsunterstütztem Video-Ident Verfahren

2.1. Generell zu Auto-Ident Verfahren

Im Zuge der aktuellen Anpassung der Online-IDV möchten wir auch die generelle Änderung der Verordnung im Hinblick auf Kundenidentifikation mittels automationsunterstütztem Video-Ident Verfahren (auch „Auto-Ident Verfahren“) anregen. Dies auch vor dem Hintergrund, dass die Änderung des Online-IDV in diesem Zusammenhang bereits schön öfters Gegenstand von Diskussionen war und leider auch die europäische Harmonisierung durch die eIDAS-VO (EU) 910/2014 zur Anerkennung von Verfahren zur Video-Identifikation nicht ausreichend ist bzw größere Lücken aufweist.
Bei Auto-Ident Verfahren wird eine Person mit ihrem entsprechenden Lichtbildausweis (zB Reisepass, Personalausweis) iSd § 6 Abs. 1 Z 1 FM-GwG mittels Videokommunikation und eines automatisationsgestützten Computerprogramms („App“) unter Abgleich von biometrischen Daten sowie einer abschließenden Ergebniskontrolle durch einen Mitarbeiter identifiziert. Zur Verwendung dieser Identifikationsmethode benötigt die Person entweder ein Smartphone oder einen Laptop mit Kamera. Es gibt bereits einige Anbieter solcher Verfahren in Europa (Onfido Limited [onfido.com], electronic identification S.L [electronicid.eu], IDnow [idnow.io]), wobei diese in vielen Fällen die höchsten Standards im Bereich IT und Datensicherheit anbieten.

2.2. Muster-Workflow eines Auto-Ident Verfahrens

Nachstehend wird beispielhaft der Workflow eines typischen Auto-Ident Verfahrens dargestellt:
Prüfung des Identifikationsdokuments: Innerhalb der App muss die Person in einem synchronen Verfahren ihren Lichtbildausweis entsprechend der Bildschirmmaske scannen, wobei der Algorithmus der App die Sicherheitsmerkmale des Lichtbildausweises überprüft sowie die Daten des Lichtbildausweises mittels OCR (Optical Character Recognition) abliest und speichert. Der Algorithmus erkennt zudem verschiedenste Betrugsschemen und Veränderungen (zB Beschädigungen, Integrität der Bildflächen, Konsistenz, Fälschungen durch Drucktechniken). Sind die Sicherheitsmerkmale des jeweiligen Dokuments nicht erfüllt und/oder werden die Daten nicht erkannt, kann die Identifikation nicht erfolgreich abgeschlossen werden.
Abgleich Foto und Person sowie Live Erkennung: Je nach Verfahren wird die Person aufgefordert unter Anwendung der Bildschirmmaske frontal in die Kamera zu schauen und ein Foto aufzunehmen (es können hierbei keine bereits existierenden Fotos verwendet werden) bzw erfolgt eine generelle Videoaufnahme der Person über die Kamera. Ohne die Involvierung einer natürlichen Person führt der Algorithmus der App einen Abgleich der biometrischen

Daten der Person mit dem Lichtbild des Ausweisdokuments durch und erkennt anhand der biometrischen Daten ob es sich um die Person auf dem Ausweisdokument handelt oder nicht. Dieses Verfahren ersetzt die menschliche visuelle Überprüfung. Zur Gewährleistung größtmöglicher Sicherheit, werden vom Programm hierbei verschiedene Sicherheitsparameter angewendet (insbesondere im Hinblick auf Betrugsversuche mit Fotos und 3D Masken von einer Person). Weiters wird die Person entweder nach dem biometrischen Abgleich der Fotos oder bereits zu Beginn des Prozesses live gefilmt. Die Person muss dabei entsprechend der Bildschirmmaske und den Anweisungen der App ihren Kopf bewegen und eine zufällig generierte Zahlenreihenfolge, die der Person synchron von der App übermittelt wird laut vorlesen. Der Algorithmus der App prüft dann wiederrum unter Anwendung technischer Sicherheitsparameter (es werden dabei unter anderem die Bewegungen sämtlicher Gesichtszüge analysiert) ob es sich um eine reale Person und ob es sich um die Person von den Fotos handelt oder nicht. Der Algorithmus erkennt durch das Live Video verschiedene Betrugsschemen (zB Kopien oder Fotos, 3D Masken, Deep Fakes, etc). Nur wenn der biometrische Abgleich der Person sowie das Live Video sämtliche Kriterien erfüllt bestätigt der Algorithmus den Abgleich der Person. Treten während des Prozesses Fehler oder Unsicherheiten auf, kann in den meisten Fällen ein Mitarbeiter hinzugezogen werden, der den Prozess prüft oder weitere Anweisungen gibt.
Prüfung durch einen Mitarbeiter und Speicherung der Daten: Die meisten Anbieter von Auto-Ident-Verfahren bieten zur Prüfung des Programms und damit zur Erfüllung des höchsten Sicherheitsstandards die Möglichkeit einer abschließenden Prüfung durch einen Mitarbeiter. Für die endgültige Bescheinigung der Identifikation muss dann der gesamte Identifikationsprozess (inklusive dem Ausweisdokument) von einem Mitarbeiter des Dienstleisters am Ende des Prozesses überprüft und entsprechend bestätigt oder abgelehnt werden. Das beim Prozess entstandene Video und der Scan des Lichtbildausweises werden vom Dienstleister aufgezeichnet und anschließend an das regulierte Institut zur Speicherung übermittelt.

2.3. Rechtliche Grundlagen

Interpretation im Rahmen der Online-IDV: Derartige Identifikationsprozesse erfüllen in vielen Fällen die inhaltlichen Anforderungen der Online-IDV, wobei die Formulierung der Online-IDV gewisse Unsicherheiten für die Anbieter birgt. Die Überprüfung des Lichtbildausweises erfolgt im ersten Schritt durch ein automationsgestütztes Computerprogramm, die Identifikation wird jedoch abschließend auch durch einen Mitarbeiter überprüft und freigegeben. Somit werden in vielen Fällen die verfahrensbezogenen Sicherheitsmaßnahmen der Online-IDV erfüllt, wobei sich allerdings im Ablauf kleine Unterschiede zur Online-IDV ergeben können. Zudem gibt es kein offizielles Anerkennungsverfahren durch eine Behörde für derartige Systeme oder eine Zertifizierungsmöglichkeit nach der Online-IDV. Dadurch gibt es Unsicherheiten bei Anbietern (insbesondere aus anderen Mitgliedstaaten) hinsichtlich der Konformität ihrer Systeme mit der Online-IDV. Aufgrund der sehr guten Eigenschaft zur Betrugserkennung solcher Algorithmen und der hohen Sicherheitsstandards sind diese aber meistens als geeignete Verfahren zu herkömmlichen Video-Identifikationsverfahren im Sinne der Online-IDV anzusehen. Der automatisierte Abgleich kombiniert mit einem ex-post Check durch geschulte Mitarbeiter bietet unsererseits jedenfalls ausreichende Sicherheit und steht dem System der klassischen Online-Identifizierung keineswegs nach.
Anbieter aus anderen Mitgliedstaaten und eIDAS-VO: Insbesondere Anbieter von Video-Identifikationsverfahren aus anderen europäischen Staaten haben es schwer durch andere Behörden anerkannt zu werden. Da es sich bei Verfahren zur Video-Identifikation nicht um Vertrauensdienste gemäß Art. 3 Z 16 VO (EU) 910/2014 handelt, ist leider der Verweis auf die Anerkennung solcher Verfahren zur Identifikation wie dies zB in § 6 Abs. 1 Z 1 FM-GwG erfolgt, nicht ausreichend. Denn bei Video-Ident Verfahren, handelt es sich um eine „elektronische Identifizierung“ iSd Art. 3 Z 1 eIDAS-VO durch Anbieter eines „Elektronischen Identifizierungssystems“ gemäß Art. 3 Z 4 eIDAS-VO und eben gerade nicht um Vertrauensdienste gemäß Art. 3 Z 16 VO (EU) 910/2014 die sich registrieren lassen können.

Zudem handelt es sich bei Anbietern von Video-Identifikationen im Normalfall um private Anbieter elektronischer Identifizierungssysteme gemäß Art. 3 Z 4 eIDAS-VO und solchen ist eine eigenständige Notifizierung ihres Systems bei der europäischen Kommission generell nicht zugänglich. Das Verfahren zur Notifizierung gemäß Art. 9 eIDAS-VO ermöglicht es ausschließlich Mitgliedstaaten elektronische Identifizierungssysteme zu notifizieren, privaten Anbietern ist das Verfahren nicht zugänglich. Gemäß der von der europäischen Kommission veröffentlichten Liste (2018/C 401/08, Anhang ./iii), hat noch kein Mitgliedstaat ein System zur Video-Identifikation notifiziert. Dementsprechend gibt es in Europa aktuell keinen Anbieter elektronische Identifizierungssysteme mittels Video-Identifikation, der bei der europäischen Kommission notifiziert ist.
Somit können sich Anbietern von Video-Identifikationen weder registrieren lassen noch ihr eigenes System an die Kommission notifizieren. Im Hinblick auf Video-Identifikationen ist ein ausschließlicher Hinweis auf die Akzeptanz von Verfahren die nach der eIDAS-VO entweder registriert oder notifiziert wurden nicht zweckdienlich und für de facto zur praktischen Unanwendbarkeit des entsprechenden Tatbestandes.
Eine Möglichkeit zur besseren Anerkennung von Anbietern von Verfahren zur Video-Identifikation aus anderen europäischen Mitgliedsstaaten wäre die Anerkennung des Verfahrens, soweit dieses die Standards der eIDAS-VO entsprechend der Durchführungsverordnung (EU) 2015/1502 erfüllt (zB bei Erfüllung des Sicherheitsniveaus „hoch“ gemäß der Durchführungsverordnung [EU] 2015/1502, Anhang Punkt 2.1.2), eventuell auch durch die Vorlage entsprechender Zertifizierungen des Anbieters. Eine weitere Möglichkeit wäre die Anerkennung des Anbieters und seines Verfahrens soweit dieses durch Behörden in einem anderen Mitgliedstaat anerkannt wurde, wobei der Nachweis in diesem Zusammenhang in vielen Ländern relativ schwierig ist.

2.4. Wirtschaftlicher Gesichtspunkte

Die meisten europäischen Staaten erkennen Verfahren zur automatisationsgestützten online Identifizierung an (zB Groß Britannien, Spanien, Liechtenstein, Luxemburg, Rumänien, etc), womit das Verfahren bereits zum neuen Standard in der FinTech-Industrie wird. Gründe hierfür sind die Sicherheit der Verfahren, die hohe Betrugserkennungsrate, die Geschwindigkeit der Identifikation sowie die wesentlich geringeren Kosten pro Identifikation. Der sehr hohe Sicherheitsstandard bei diesen Verfahren wird durch immer bessere Algorithmen im Bereich Text- und Bilderkennung (meist mithilfe von Deep-Learning) gewährleistet. Dafür spricht auch, dass im Bereich der Betrugserkennung immer mehr automatisierte Programme zum Einsatz kommen, da diese Daten und Muster wesentlich schneller erkennen und abgleichen können. Als zusätzliche Sicherheitsstufe, um die Ergebnisse solcher Programme zu überprüfen, werden Identifikationen dann noch von einem Mitarbeiter nachvollzogen und abschließend bestätigt. Da herkömmliche Verfahren faktisch kein höheres Sicherheitsniveau bieten als die beschriebene Methode des Auto-Ident Verfahrens, gibt es aus unserer Perspektive keine objektivierbare Rechtfertigung dafür, dass Auto-Ident Verfahren welche den höchsten Sicherheitsstandard bieten nicht auch in Österreich anerkannt werden. Eine fehlende offizielle Anerkennung des Auto-Ident Verfahren, stellt für Unternehmen, welche auf derartige Identifikationsverfahren angewiesen sind, einen signifikanten Wettbewerbsnachteil im europäischen Kontext dar.

3. Ansuchen

Aus den genannten Gründen wäre eine Anpassung der Online-IDV zur Akzeptanz von Auto-Ident-Verfahren unter der Vorgabe gewisser Standards unseres Erachtens angemessen und hilfreich. Ein solcher Schritt kann auch generell in der FinTech-Industrie einen wichtigen Beitrag zur Verbesserung der Kundenzufriedenheit und der Kosten von Produkten leisten, was sich entsprechend auf den Wettbewerb auswirken kann. Gerade auch im Zusammenhang mit der erzwungenen Umstellung auf rein digitale Konzepte durch die Situation mit der COVID-19 Pandemie, zeigt sich die enorme Effizienz, Praktikabilität und Sicherheit von rein digitalen

Lösungen. Dementsprechend würden wir eine Anpassung/Neuregelung der Online-IDV sowohl bezüglich der generellen Homeoffice Lösung aber insbesondere im Hinblick auf die Anerkennung von Auto-Ident-Verfahren sehr begrüßen.

Freundliche Grüße

FACHVERBAND FINANZDIENSTLEISTER

Mag. Hannes Dolzer
Fachverbandsobmann

Mag. Thomas Moth
Geschäftsführer