



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
02.06.2021

Stellungnahme des Fachverbands Finanzdienstleister zum Entwurf der Verordnung der Finanzmarktaufsichtsbehörde (FMA), mit der die Online-Identifikationsverordnung geändert wird

Der Fachverband Finanzdienstleister bedankt sich für die Gelegenheit zur Stellungnahme im Rahmen des Begutachtungsverfahrens.

I. Einleitung

Wir begrüßen den Schritt der Finanzmarktaufsichtsbehörde, Finanzinstituten im Rahmen der Geldwäscheprävention gemäß FM-GwG die Nutzung moderner und sicherer Verifizierungslösungen zur Identifikation ihrer Kunden (KYC) zu ermöglichen.

Bereits vor COVID-19 war ein deutlicher Trend zur digitalisierten Begründung einer Geschäftsbeziehung vorhanden. Durch die Pandemie wurde dieser noch beschleunigt. Insofern ist es sinnvoll und nützlich Kunden und Dienstleister durch geeignete Methoden zur Fernidentifizierung zu unterstützen.

Nichtsdestotrotz glauben wir, dass der vorgeschlagene Entwurf noch punktuell Verbesserungspotenzial besitzt. Dieses möchten wir mit unseren Anmerkungen näher ausführen.

II. Im Detail

Zu § 4 Abs. 3 Z 2:

Die Bestimmung dient dazu den Anbietern eine Überprüfung der tatsächlichen Anwesenheit einer Person (liveness-check) bei der Identifizierung zu verifizieren. Vor dem Hintergrund, dass der Großteil der Identifizierungen über Mobiltelefon erfolgt, erscheint eine Mindestanzahl an acht Zeichen aus praktischen Überlegungen und Platzgründen für zu hoch gegriffen. Zudem macht es sicherheitstechnisch keinen Unterschied, wie viele Zeichen abgefragt werden.

Wir regen daher an, die erforderliche Mindestanzahl an Zeichen auf drei zu beschränken:

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

Zu § 4 Abs. 6 Z 1:

Es steht außer Zweifel, dass der Verpflichtete sicherstellen muss, dass seine im Einsatz befindlichen biometrischen Identifikationsverfahren laufend dem aktuellen Stand der Technik entsprechen. Gleichwohl sind wir der Meinung, dass das Setzen „aktiver Überwachungsmaßnahmen“ die Technologieneutralität gefährdet, indem es aktive (menschliche) Maßnahmen impliziert.

Im Sinne einer neutraleren Wortfolge schlagen wir vor das Wort „aktiv“ in Anlehnung an § 6 Abs. 1 Z 2 FM-GwG („*angemessener Maßnahmen zur Überprüfung seiner Identität*“) durch das Wort „angemessen“ zu ersetzen:

„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 **aktiverangemessener** Überwachungsmaßnahmen, um etwaige Probleme unmittelbar zu erkennen und zu beseitigen.“

Zu § 6 Abs. 5:

Der Vorschlag, NFC-basierte Identifizierungen für eine remote-Identifikation einzusetzen ist gut, beinhaltet als alleinige und bedingungslose Ergänzung allerdings etliche Nachteile und Risiken für die Verpflichteten und ihre Kunden.

Insbesondere vor dem Hintergrund eines risk-based approach, wie ihn die EBA in ihren Leitlinien fordert, erscheint die Festlegung einer NFC-basierten Identifizierung zu absolut:

“33. Given the above, the EBA reminds CAs that they have to apply a risk-based approach to AML/CFT supervision under Article 48 of the AMLD. Furthermore, in line with Article 16 of the EBA’s founding Regulation, CAs have a legal duty to make every effort to comply with EBA’s Risk-based Supervision Guidelines. While these Guidelines are being updated, CAs are expected to have considered the recommendations set out in the EBA’s report on competent authorities’ approaches to the AML/CFT supervision of banks.”

Um den Verordnungsgeber bestmöglich zu unterstützen, haben wir versucht, die Vor- und Nachteile von NFC kurz und übersichtlich darzulegen:

Vorteil:

- Zusätzliche Überprüfung der Zertifikate, stärkere Sicherheitsmerkmale

Nachteile:

- Bestehende Systeme und Prozesse passen nicht dazu (EBA führt in ihren Leitlinien aus, dass auf bestehende Prozesse Rücksicht genommen werden soll).
- NFC benötigt zwingend eine native App, der Trend geht allerdings gegen neue Individualapps, zumal die überwältigende Mehrheit der österreichischen Finanzinstitute ihre Antragsstrecken web- und nicht app-basiert haben.
- In manchen Ländern sind über 50% aller Zertifikate gültiger Reisepässe revoked. Das Dokument ist aber weiterhin gültig. Das führt zu Vorverurteilung und Einschüchterung der Kunden.
- Biometrische Ausweisdokumente - mit Ausnahme der Reisepässe - kommen in der Praxis (noch) nicht flächendeckend zum Einsatz. Dies trifft insbesondere auf die Vielzahl von national unterschiedlichen Personalausweisen (auch innerhalb der EU) zu. Wengleich mittlerweile auch neu ausgestellte Personalausweise teilweise mit NFC Chip ausgestattet werden, muss zusätzlich die durchschnittliche Gültigkeitsdauer (idR 10 Jahre) von Personalausweisen in Betracht gezogen werden, weshalb der Großteil

der aktuell noch im „Umlauf“ befindlichen und nach FM-GwG zulässigen Lichtbildausweise keine elektronisch gespeicherten Daten vorweisen.

- Zusätzlich können wir durch die Europa-weite geringe Nutzung von NFC-Chips in ID-Karten außerhalb Österreichs annehmen, dass mittlerweile eine große Bevölkerungsgruppe in Österreich, die nicht Österreicher sind (17,1% laut Statistik Austria), in Gefahr laufen vom Österreichischen Finanzmarkt ausgeschlossen werden.

Im Ergebnis zeigt sich: Auch NFC ist limitiert. Es setzt ein bestimmtes Smartphone-level voraus, funktioniert ausschließlich in nativen Applikationen - also nicht auf den momentanen Antragsstrecken der Finanzdienstleister, funktioniert auf absehbare Sicht nur mit europäischen Reisepässen bzw. Wenigen ID-Karten und gibt keine verlässliche Auskunft über die Gültigkeit (sehr wohl aber die Authentizität) eines Ausweises.

Die Verordnung geht unserer Ansicht daher zu kurz, da hier ein großer Teil der in Österreich lebenden Bevölkerung und auch viele Finanzinstitute von einer Nutzung dieser Identifizierungslösung ausgeschlossen wird.

Wir regen daher die zusätzliche Aufnahme weiterer, zeitgemäßer und ebenso sicherer Identifikationsalternativen als Stand der Technik an.

Unsere Vorschläge:

Neben der im Verordnungsentwurf vorgeschlagenen Erweiterung durch die NFC Identifizierung sollen zusätzlich Möglichkeiten je nach “Stand der Technik” im Zuge eines risikobasierten Ansatzes und einem Transaktionsmonitoring bei erhöhtem Risiko erweitert und kombiniert werden mit:

- Verbesserte Referenzüberweisung - bestehender je nach Risikoabschätzung ergänzt durch:
 - o Photoidentifizierung - eine Photoidentifizierung kann durch Verwendung bestimmter Services leicht auf das Sicherheitsniveau einer NFC-Identifizierung gebracht werden. Es gibt zugegebenermaßen nur wenige Services, die verlässlich die optischen Sicherheitsmerkmale sicher verifizieren können. (Ausweisverifizierung und Fälschungserkennung durch Analyse aller mit einer Smartphone-Kamera verwertbaren Sicherheitsmerkmale, biometrischer Abgleich und Lebenderkennung mit sichereren Verfahren als den gestenbasierten.)
 - o Adressverifizierung (programmatische Überprüfung, ob eine Person tatsächlich an einer Adresse wohnt)
 - o PSD2-Login mit Kontoinformationsdienstleister (Als Ersatz der Referenzüberweisung, die keinerlei Mehrwert in der Feststellung des Kontoinhabers hat bzw weniger Aussagekraft als das real-time-login)
- Gehärtete Photoidentifizierung - bestehend je nach Risikoabschätzung ergänzt durch:
 - o Photoidentifizierung, aber zusätzlich weitere Sicherungsmaßnahmen, etwa:
 - o Mobile Identification (zumindest Name, Mobilfunknummer, Nationalität und aktueller Besitz des Geräts)
 - o Gegebenenfalls risikobasiert:
 - Adressverifizierung
 - Überprüfung gegen Account Takeover und anderer Risikofaktoren
- Risikobasierte sichere Photoidentifizierung - bestehend je nach Risikoabschätzung ergänzt durch:
 - o Eine Photoidentifizierung ist nachgewiesenermaßen einer Begutachtung durch geschulte Personen überlegen und kann nicht ermüden. Wir unterstützen diese

Aussage und schlagen vor, eine automatisierte Variante der Personalsichtung für risikoarme Situation als ausreichend zu erachten.

Zu § 9 Abs. 2:

Für den Fall, dass - entgegen unserer Ausführungen - an der NFC-basierten Identifizierung alternativlos festgehalten wird, regen wir eine Verlängerung der vorgeschlagenen Übergangsfrist von 31. März 2022 bis zum **31. Dezember 2022** an.

Es gilt zusätzlich zu den vorgenannten Überlegungen folgende Punkte zu beachten, die für eine entsprechend längere Übergangsfrist sprechen, in der auch weiterhin eine „optische“ Überprüfung der Echtheit des Lichtbildausweises nach § 4 Abs. 4 Z 1 bis 5 zulässig ist:

Für die Vornahme der notwendigen Umstellungen und Sicherstellung der Integrität der technischen Prozesse für die automatische Auslesen und Überprüfen von elektronisch gespeicherten Daten und die damit einhergehende Anpassung der Geschäftsmodelle von (Finanz-)Dienstleistern sollte eine längere Frist als 9 Monate vorgesehen werden.

Das gilt insbesondere auch vor dem Hintergrund der geplanten Überarbeitung der eIDAS-VO und künftigen EU e-ID (Veröffentlichung am 2. Juni 2021 geplant). Eine längere Frist würde (Finanz-)Dienstleistern die Möglichkeit geben allfällige Neuerungen in diesem Bereich bereits im Rahmen der Umstellung auf die Online-IDV mit zu berücksichtigen.

(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~~ **Dezember** 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.“

Für Rückfragen stehen wir jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen

FACHVERBAND FINANZDIENSTLEISTER



KommR Mag. Hannes Dolzer
Fachverbandsobmann



Mag. Thomas Moth
Geschäftsführer