REDEN WIR ÜBER AUFSICHT

KOMPLEXE VORGABEN.
KLARE ERWARTUNGEN.

FMA

Identifizierung im Ferngeschäft

Technologische Entwicklungen ändern die Rahmenbedingungen bei der Geldwäscheprävention.

Für die Prävention von Geldwäscherei und Terrorismusfinanzierung (GW/TF) zeigt sich dies beispielsweise bei online Geschäftsabschlüssen. Die eindeutige und sichere Identifizierung von Kund:innen stellt – als Teilbereich des sogenannten Know-Your-Customer-Prinzips (KYC) – eine zentrale Maßnahme zur Prävention von GW/TF dar.

Ausgangslage

Würde ein Verpflichteter nicht genau wissen, »wer« die Kund:innen bzw. handelnden Personen sind, mit denen er Geschäfte macht (machen möchte), etwa weil die Identifizierung anhand von untauglichen oder gar gefälschten Dokumenten erfolgt ist, würde dies sein Risiko, für Zwecke der GW/TF missbraucht zu werden, exorbitant erhöhen. Deshalb gibt es im Bereich der Identifizierung unabhängig von der Risikoklasse der jeweiligen Einzelkund:innen besonders detaillierte Vorgaben zu beachten. Das FM-GwG geht bei der Feststellung und Überprüfung der Identität von Kund:innen (und Vertretungsbefugten) grundsätzlich von der persönlichen Vorlage des amtlichen Lichtbildausweises aus. Das FM-GwG erlaubt den Ersatz der persönlichen Vorlage des Ausweises bei Geschäftsbeziehungen oder Transaktionen ohne persönliche Kontakte (Ferngeschäft) nur durch gesetzlich normierte Sicherungsmaßnahmen, die das Risiko aus dem fehlenden unmittelbaren Kundenkontakt – etwa den Einsatz von gefälschten Ausweisdokumenten –, mitigieren sollen. Das FM-GwG kennt vier alternative Sicherungsmaßnahmen:

- die **Online-Identifikation,** also die Vorlage des amtlichen Lichtbildausweises im Rahmen eines videogestützten elektronischen Verfahrens gemäß den organisatorischen und prozessualen Vorgaben der FMA-Online-Identifikationsverordnung;

§ **§ 6 Abs 4 FM-GwG** regelt die alternativen Sicherungsmaßnahmen zum Ersatz der persönlichen Vorlage des amtlichen Lichtbildausweises

- die Verwendung eines **elektronischen Ausweises** auf Basis eines gesetzlich vorgesehenen Verfahrens, das gesichert dieselbe Information wie mit der Vorlage eines amtlichen Lichtbildausweises zur Verfügung stellt, wobei insbesondere auf eine revisionssichere Speicherung der Identifikationsdaten zu achten ist (etwa die ID-Austria in Vollfunktion);
- die Abgabe der **rechtsgeschäftlichen Erklärung** der Kund:innen in Form einer qualifizierten elektronischen Signatur oder die Zustellung der rechtsgeschäftlichen Erklärung des Verpflichteten mit eingeschriebener Postzustellung an den Wohnsitz / Sitz der Kund:innen, wobei – je nachdem, ob es sich um eine natürliche oder juristische Person handelt – zusätzlich eine schriftliche Erklärung betreffend den Hauptsitz der Verwaltung bzw. Ausweiskopien der Kund:innen / der Vertretungsbefugten erforderlich sind und, sofern es sich um eine:n Kund:in mit Sitz in einem Drittland handelt, noch zusätzliche Vorgaben bestehen.
- die **Referenzkontomethode,** bei der die erste Zahlung einer Transaktion über ein Konto abgewickelt werden muss, das auf den Namen der Kund:innen bei einem »qualifizierten Dritten« gemäß FM-GwG eröffnet wurde und zusätzlich aussagekräftige Kopien von Dokumenten der Kund:innen vorliegen oder eine schriftliche Bestätigung des qualifizierten Dritten.

Alle Sicherungsmaßnahmen gemäß FM-GwG weisen als Gemeinsamkeit auf, dass ein alleiniges Einholen von (Ausweis-) Kopien, sei es physisch oder elektronisch, niemals ausreichend ist. Vielmehr sind abhängig von der gewählten Variante die spezifisch normierten prozessualen Vorgaben zu erfüllen, um das aus dem fehlenden unmittelbaren Kundenkontakt resultierende Risiko zu mitigieren. Praktische Probleme ergeben sich oftmals bspw. wenn unterschiedliche Sicherungsmaßnahmen vermischt oder Elemente unterschiedlicher Sicherungsmaßnahmen – entgegen der gesetzlichen Vorgabe – kombiniert werden. Die konkrete Einhaltung der jeweiligen Sicherungsmaßnahme im Ferngeschäft und die Angemessenheit der dabei von den Verpflichteten gesetzten Kontrollen und Maßnahmen ist zu dokumentieren und der FMA, bspw. im Rahmen von Vor-Ort- oder anderen Aufsichtsmaßnahmen nachzuweisen.

▶ **Risikoanalyse**
Die Möglichkeit von Geschäftsabschlüssen im Ferngeschäft und risikomitigierende Maßnahmen sind gemäß § 4 Abs 1 FM-GwG jedenfalls in der Risikoanalyse der Verpflichteten abzubilden.

Neue Technologien im Identifizierungsprozess

Die Frage, inwiefern neue Technologien – auch im Rahmen der Identifizierung – eingesetzt werden, bildet aber auch einen zentralen Bestandteil des institutsspezifischen Geschäftsmodells und ist in der Risikoanalyse auf Unternehmensebene zu berücksichtigen. Die Online-Identifikation ermöglicht den Identifizierungsprozess gemäß der FMA-Online-Identifikationsverordnung. Dabei stehen neben der Datenqualität und -sicherheit vor allem auch die Aspekte der Fälschungs- und Missbrauchssicherheit sowie eine technisch gesicherte Übertragung im Vordergrund. Leider zeigt sich immer wieder, dass der Einsatz gefälschter Identifizierungsdokumente trotz aller technischer Vorkehrungen im digitalisierten Alltag keine Seltenheit ist. Ein besonders sorgfältiger Umgang mit neuen Technologien ist daher unabdingbar.

Verpflichtete des FM-GwG haben bei der Nutzung von Online-Identifikationsverfahren gemäß FM-GwG bzw. Online-IDV der FMA eine Reihe von Vorsichtsmaßnahmen zu treffen, um sicherzustellen, dass

▶ **»Purple Notice«**
Die A-FIU veröffentlichte am 22. März 2024 mittels goAML eine sogenannte »purple notice«, in der sie darauf hinweist, dass die Anzahl von totalgefälschten Identitätsdokumenten speziell bei Online-Identifikationsverfahren stark zugenommen hat.

die Identifizierung ordnungsgemäß und sicher durchgeführt wird. Zentrale Aspekte bilden dabei zunächst ein hohes Maß an Sorgfalt bei der Implementierung (eigener) technischer Lösungen, bei der Auswahl von externen Dienstleistern sowie bei der angemessenen vertraglichen Gestaltung von Kooperations- bzw. Auslagerungsvereinbarungen. Klar dokumentiert und der FMA gegenüber nachweisbar muss unabhängig von dem gewählten Vorgehen sein, wer wofür konkret zuständig ist und wie im Zusammenwirken die gesetzlichen Vorgaben angemessen eingehalten werden. Ungeachtet, ob es sich bei dem Kooperationspartner um einen qualifizierten Dritten oder einen externen Dienstleister handelt, ist sicherzustellen, dass die Kontroll- und Überprüfungsmöglichkeiten der FMA dadurch nicht behindert werden.
Zu beachten gilt weiters, dass die Verantwortung für die Einhaltung der Vorgaben des FM-GwG letztlich bei jedem einzelnen Verpflichteten bleibt. Von den Verpflichteten sind routinemäßig Kontrollhandlungen durchzuführen, um potenzielle Risiken und Schwachstellen frühzeitig zu erkennen. Zu denken ist dabei anhand des Beispiels eines externen Dienstleisters u. a. an folgende Kontrollmaßnahmen:

- Verpflichtete müssen die **Einhaltung der gesetzlichen Bestimmungen** sicherstellen und sich vergewissern, dass der ausgewählte Dienstleister die einschlägigen gesetzlichen Bestimmungen ebenfalls einhält.
- Verpflichtete müssen prüfen, ob der gewählte externe Dienstleister die erforderlichen **Userdaten der zu identifizierenden Person** vorliegen hat. Die Auslagerungsvereinbarung zwischen externem Dienstleister und Verpflichteten muss ausreichend **Einsichtsrechte** in die gesammelten Informationen, Daten und Dokumente vorsehen. Zudem ist eine Feedback-Schleife zwischen den externen Dienstleistern und den Verpflichteten einzurichten, um den Online-Identifikationsprozess an die sich stets ändernden Gefahrenlagen adäquat und rasch anpassen zu können.
- Verpflichtete müssen prüfen, ob der externe Dienstleister während der Identifikation einer zu identifizierenden Person eine **Audiodatei** aufzeichnet und ob diese klar und deutlich ist. Es muss sichergestellt sein, dass während des Identifizierungsprozesses entsprechende **Bildschirmkopien** vom externen Dienstleister erstellt werden, die den Ablauf der Identifizierung dokumentieren. Verpflichtete haben sich von der ordnungsgemäßen Dokumentation zu überzeugen.
- Die externen Dienstleister sowie die Verpflichteten haben zu prüfen, ob die zu **identifizierende Person allein** im Video zu sehen ist oder ob andere/mehrere Personen erkennbar sind. Es gilt sicherzustellen, dass die Identifizierung nicht von Dritten beeinflusst wird.
- Es muss geprüft werden, ob die **Angaben zur Person** (insbesondere in Bezug auf Alter und Identität) mit dem **Kopfbild** der zu identifizierenden Person **übereinstimmen.**
- Der externe Dienstleister muss gegebenenfalls **zusätzliche Sicherheits-Tools** einsetzen, wie etwa spezielle Programme zur Dokumentenprüfung, um eventuelle Manipulationen der vorgelegten Ausweisdokumente zu erkennen.
- Verpflichtete müssen zudem überprüfen, ob der externe Dienstleister **»Device-Fingerprinting«** verwendet, um sicherzustellen, dass die Angaben der zu identifizierenden Person bspw. betreffend den Wohnort mit den tatsäch-

▶ Die umfangreichen organisatorischen und prozessualen Vorgaben werden der FMA-Onlineidentifikationsverordnung und dem einschlägigen FMA-Rundschreiben »Sorgfaltspflichten zur Prävention von GW/TF« dargestellt.

lichen Log-in-Daten des verwendeten Geräts übereinstimmen, um etwaige betrügerischen Aktivitäten frühzeitig erkennen zu können.

Ist die visuelle Überprüfung von potentiellen Kund:innen, seiner vertretungsbefugten natürlichen Person und/oder des jeweiligen amtlichen Lichtbildausweises nicht möglich, ist die Online-Identifikation abzubrechen.
Eine derartige Unmöglichkeit kann sich zum Beispiel aufgrund schlechter Lichtverhältnisse, einer schlechten Bildqualität, einer schlechten Bildübertragung oder eines technischen Defekts ergeben. Treten anderweitige Unstimmigkeiten wie Störungen der sprachlichen Kommunikation oder sonstige technische Gebrechen auf, so ist auch in diesen Fällen ein Abbruch der Online-Identifikation durchzuführen, wenn diese Unstimmigkeiten nicht nachvollziehbar sind bzw. zweifelsfrei aufgeklärt werden können. Seitens der Verpflichteten sind dabei jedenfalls die Rechtsfolgen des § 7 Abs 7 FM-GwG zu beachten.

§ **§ 5 Online-Identifikationsverordnung** regelt den zwingenden Abbruch der Online-Identifikation.

Conclusio und Ausblick

Die Identifizierung der Kund:innen im Fern- bzw. Onlinegeschäft birgt sowohl Chancen als auch Risiken. Um den damit verbundenen Risiken entsprechend entgegenzuwirken, ist es für Verpflichtete unabdingbar, sich mit den gesetzlichen Vorgaben auseinanderzusetzen und großes Augenmerk auf die sachgerechte Auswahl von Kooperationspartnern bzw. externen Dienstleistern sowie auf klare Vereinbarungen und Leistungspakete zu legen.
Ebenso zentraler Stellenwert kommt internen Qualitäts- und »Second-Level«-Kontrollen zu, um die Risiken wie Totalfälschungen von Ausweisdokumenten und damit verbundene, evidente Reputations- und Missbrauchsrisiken möglichst effektiv zu mitigieren.
Die Verantwortung für die Einhaltung der gesetzlichen Vorgaben bleibt letztlich, ungeachtet der gewählten Vorgehensweise/Sicherungsmaßnahme und losgelöst davon, ob der Identifizierungsprozess über qualifizierte Dritte oder externe Dienstleister erfolgt, stets bei jedem einzelnen Verpflichteten.

▶ **Ausblick:**
Künftig werden in Bezug auf die Online-Identifikation noch strengere Regeln gelten: Sie wird an die Voraussetzungen der eIDAS-Verordnung (EU) 910/2014 geknüpft werden. Diese Anforderungen dürften über Technische Regulierungsstandards (RTS) der AMLA ergänzt bzw. konkretisiert werden.

Link

Weitere Informationen zur Prävention von Geldwäscherei und Terrorismusfinanzierung finden sie auf der Website der FMA:
www.fma.gv.at → Aufsicht → Querschnittsthemen → GW/TF

§ Wir stützen unsere Aussagen auf teils komplexe rechtliche Vorgaben, die wir am Rand ausweisen, oder leiten sie davon ab, ohne neues Recht zu schaffen, so dass über die gesetzlichen Bestimmungen hinausgehende Rechte und Pflichten hieraus nicht abgeleitet werden können. Wir formulieren klare Erwartungshaltungen, die sich weitestmöglich auf Rechtsprechung und europäische Auslegungshilfen stützen, i. Ü. aber unsere eigene fachkundige Rechtsauffassung wiedergeben. Wir gehen mit der Zeit, weswegen wir uns die Aktualisierung der angeführten Orientierungshilfen jederzeit vorbehalten.
Obige Aufzählungen stellen keine abschließende Liste dar und sind jedenfalls nur ergänzend und klarstellend zu betrachten.