Onfido GmbH - c/o Osborne Clarke,
Innere KanalstraBe 15,
50823, Koln

An Finanzmarkaufsichtsbehörde.
Otto-Wagner-Platz 5,
A-1090 Wien
per Email an begutachtung@fma.gv.at

4. Juni 2021

BETREFF: Stellungnahme zur Begutachtung einer Verordnung zur Änderung der Online Identifikationsverordnung/GZ: FMA-LE0001.210/0007-INT/2021

Sehr geehrte Damen und Herren!

Onfido, Anbieter von Softwarelösungen für digitale Identitätsprüfung und Authentifizierung, begrüßt die Novellierung der Online-Identifikationsverordnung zur Erweiterung der Online-Identifikation um biometrische Identifikationsverfahren.

Digitale Identitätsverifizierung bringt Unternehmen eindeutigen wirtschaftlichen Nutzen und erhöht ihre Wettbewerbsfähigkeit, indem sie Kundenbeziehungen stärkt und neue Geschäftsmodelle ermöglicht. Die Evolution digitaler Identifikationsmethoden, insbesondere unter Verwendung von Künstlicher Intelligenz, verbessert nicht nur bestehende Technologien in puncto Effizienz, sondern erhöht auch ihre Sicherheit und Robustheit, um den ständig wachsenden Anforderungen gerecht zu werden. Denn da immer mehr Services online angeboten werden, nehmen auch Cybersecurity-Bedrohungen und Herausforderungen in Bezug auf Sicherheit, Datenschutz, Benutzererfahrung und Compliance zu. Digitale Lösungen sind dabei gleichzeitig effizient, praktikabel und sicher.

Wir setzen uns für einen regulativen Rahmen mit technologieneutralen Anforderungen und Standards an das biometrische Identifikationsverfahren ein. Wir sind der festen Überzeugung, dass Sicherheit und Innovation sich nicht widersprechen, sondern sich gegenseitig verstärken und daher kein Hindernis für zukunftsgerichtete Regulierung darstellen.

Onfido Ltd is registered with the Information Commissioner under the terms of the Data Protection Act 1998

Onfido bedankt sich für die Möglichkeit, zum Begutachtungsentwurf der Online-IDV Stellung nehmen zu können und darf folgende Kommentare weitergeben:

2. Teil/Sicherungsmaßnahmen/Verfahrensbezogene Sicherungsmaßnahmen: Mitteilung einer mindestens acht Zeichen umfassende Zeichen- oder Wortfolge während der Online-Identifikation (§ 4 Abs. 3 Z 2)

Forschung zur User Experience zeigt, dass 45% aller Personen eine Identitätsprüfung aufgrund von schlechter Benutzererfahrung abbrechen. Die Wiederholung bestimmter Teile des Prozesses infolge von menschlichen Fehlern wie Schreibfehlern ist eine besonders große Schwachstelle, das Potenzial für menschliche Fehler steigt mit der Länge der Sequenz oder Anzahl der Zeichen. Reibungsverluste sollten aber so gering wie möglich gehalten werden, um die Liveness und Identität einer Person zuverlässig und sicher zu überprüfen. Modernste Technologie kann bereits jetzt den Liveness Check durch viel kürzere, zuverlässigere und benutzerfreundlichere Methoden wie zufällige Kopfbewegungen oder eine Folge von nur 3 zufällig generierten Zahlen sicher überprüfen. Wir regen daher die Verpflichtung einer mindestens drei Zeichen umfassende Zeichen- oder Wortfolge an, um die falsche Rückweisungsrate, die bei 8 Zeichen auftreten würde, zu reduzieren.

**Referenz: FMA Handout Feb 2021, Folien 17; 22 – 27*

2. Teil/Sicherungsmaßnahmen/Verfahrensbezogene Sicherungsmaßnahmen: Verpflichtung Aufnahmen, die zum Zwecke der Online-Identifikation erstellt werden, in ihrer Gesamtheit akustisch und optisch aufzuzeichnen (§ 4, Abs. 6, Z 2)

Wohingegen die akustische Aufzeichnung während Live-Interaktionen und deren Speicherung zur Überprüfbarkeit durchaus sinnvoll ist, gilt dies weniger für biometrische Verfahren. Automatisierte Methoden am neuesten Stand der Technik, wie Lippensynchronisation und

Sprache-zu-Text-Technologien ermöglichen es Verifikationssystemen, Liveness ohne akustische Aufzeichnungen effizient und sicher zu prüfen. Künstliche Intelligenz kann bereits jetzt biometrische Daten durch Lippenerkennung und Synchronisierung mit einer 3-teiligen Sequenz an Bewegungen viel effizienter verarbeiten. Untersuchungen zeigen, dass Gesichtsabgleich-Algorithmen eine Fehlerrate von weniger als 0,1% aufweisen,

während Menschen eine Fehlerrate von 14 % beim Vergleichen von unbekannten Gesichtern aufweisen.

**Referenz: FMA Handout Feb 2021, Folien 10 - 13; 27)*

2. Teil/Sicherungsmaßnahmen/Verfahrensbezogene Sicherungsmaßnahmen: Für Biometrische Identifikationsverfahren dürfen nur Lichtbildausweise, deren Inhalt von der ausstellenden Behörde elektronisch signiert worden ist, verwendet werden. (§ 4, Abs. 6, Z 5)

Derzeit ist nur eine begrenzte Anzahl von Dokumenten in der Lage, elektronisch signierte Daten über NFC bereitzustellen. RFID-Chips sind nicht in jedem Reisepass enthalten, geschweige denn in jedem derzeit im Umlauf befindlichen Ausweisdokument. Sie können zudem beschädigt sein oder aus anderen Gründen nicht gelesen werden. Eine Beschränkung der Verwendung auf allein diese Dokumente würde die Effektivität der automatisierten Verarbeitung drastisch einschränken.

Zudem wurde die NFC-Authentifizierung nicht mit Blick auf die Remote-Verifizierung entwickelt, sondern hauptsächlich für das grenzüberschreitende Reisen mit e-Gates. Bei einer physischen Identitätsüberprüfung bei der Grenzkontrolle wird mit dem Auflegen des Dokuments auf ein Passlesegerät oder E-Gate das Dokument und der Chip gleichzeitig unter zusätzlicher Kontrolle durch Grenzbeamte bewertet, um so Missbrauch und Betrug zu verhindern. In der Remote-Umgebung sieht man das Dokument beim Zugriff auf den Chip nicht, daher besteht immer die Möglichkeit, dass ein anderes Gerät anstelle eines tatsächlichen Chips verwendet wird, um die Chipantworten zu simulieren und zu fälschen.

Wo elektronisch signierte Daten nicht verfügbar sind, können mit modernsten OCR-Methoden (Optical Character Recognition) Daten aus dem Körper und/oder MRZ eines Dokuments extrahiert werden. Zusätzlich werden Dokumente gegen “Templates”, die korrekte Form, Format und Struktur vorgeben, sowie verschiedenste Sicherheitsmerkmale wie Wasserzeichen, Hologramme, Tinten und Aufdrucke mit verschiedensten Charakteristiken (reflektierend, relief, Farbänderung) verglichen und geprüft. Die extrahierten Daten werden ebenfalls mit den verschlüsselten Daten aus der Machine Readable Zone (MRZ, 2 - 3 Zeilen die in der Regel viele >>>>> beinhalten) abgeglichen, um die interne logische Datenkonsistenz sicher zu stellen.

Onfido ist überzeugt davon, dass digitale Identitätsverifizierung unter den aufgeführten Bedingungen eines regulativen Rahmens mit technologieneutralen Anforderungen und Standards eine Bereicherung für Unternehmen und ihre Kunden sein kann.

Gerne stehen wir für Rückfragen und weiteren Input jederzeit zur Verfügung.

Mit freundlichen Grüßen,

Oliver Krebs

Vice President Central EMEA

Onfido

Onfido Ltd is registered with the Information Commissioner under the terms of the Data Protection Act 1998