Stellungnahme zur Verordnung
zur geldwäscherechtlichen Identifizierung durch Videoidentifizierung
(Geldwäschevideoidentifizierungsverordnung – GwVideoIdentV)

Die Digitalisierung des deutschen Finanzsektors ist ein **zentraler Wettbewerbsfaktor**, um im europäischen und globalen Wettbewerb zu bestehen. Insbesondere die Nutzung **technischer Innovationen im Identifizierungsprozess** von Neukunden trägt dazu bei, die Attraktivität der Finanzinstitute und damit des Standortes Deutschland insgesamt zu stärken.

Identifizierungsverfahren wie die agentengestützte Video-Identifizierung oder eID haben aufgrund **nutzerunfreundlicher Prozesse, hoher Kosten oder geringer Verbreitung bisher nur bedingt zur Wettbewerbsfähigkeit des deutschen Finanzsektors in der EU beigetragen. Im EU-Ausland, etwa in Spanien oder Österreich, bringen innovative Identifizierungsverfahren die Digitalisierung des Finanzsektors jedoch schon länger maßgeblich voran.**

Wir begrüßen deshalb, dass das Bundesministerium der Finanzen mit der Veröffentlichung einer **Verordnung zur geldwäscherechtlichen Identifizierung durch Videoidentifizierung** den Markt für **hochinnovative und automatisierte Ident-Verfahren** öffnet.

Solche Identifizierungsverfahren bieten die Möglichkeit, **schnell, sicher und nutzerfreundlich alltägliche und für Bürger:innen hochrelevante Vorgänge wie** Kontoeröffnungen bzw. Onboardings durchzuführen. Außerdem bieten sie **kostengünstigere Identifizierungsprozesse für Banken** und steigern nachweislich die Sicherheit gegenüber einer rein menschlichen Kontrolle.

Automatisierte Ident-Verfahren sind zudem **eine Ergänzung zum Online-Ausweis (eID)**. In der Privatwirtschaft hat sich bewiesen, dass eine Gesamtlösung aus eID und sicheren Alternativen **ökonomisch effizient ist und der eID-Verbreitung hilft.** Das Self-Service-Verfahren der automatisierten Video-Identifizierung eignet sich zudem, um die Nutzenden bei Herausforderungen im eID-Prozess (z. B. fehlende PIN) nahtlos in das automatisierte Video-Ident zurückzuführen. **Dies führt zu höherer Akzeptanz bei Instituten, auch die eID-Funktion anzubieten**, weil eine hohe Erfolgsrate gewährleistet ist.

Um eine reibungslose Anwendung der Verordnung zu gewährleisten und geplante Regelungen klarer zu gestalten, sehen wir jedoch weiteren Änderungsbedarf in §9, §§ 10 und 11 sowie §16 und §17 für die teil- und vollautomatisierten Verfahren.

Zu §9

- Um eine gute Bildqualität und einen wesentlich größeren Schutz gegen das Injizieren von verfälschten Bildern zu gewährleisten, ist in der Gesetzesbegründung dringend anzuraten, dass Video-Identifizierungsverfahren ausschließlich mittels einer nativen App und nicht in einem Browser durchgeführt werden dürfen. Hierdurch wird auch die gleichwertige Nutzung zur eID bekräftigt, da diese auch eine App benötigt.

Zu §10 und §11

- Die §§ 10 und 11 würden eine konforme optische Fernidentifizierung von Ausweisdokumenten praktisch unmöglich machen, da die Anforderungen nicht in der Praxis umsetzbar sind.
- Wir raten dringend dazu, die Anforderungen aus dem Rundscheiben 3/2017 hinsichtlich der Ausweisprüfung zu übernehmen.

Zu §14

- In der Gesetzesbegründung zu §14 wird der Einsatz von automatisierten, softwarebasierten Werkzeugen, basierend auf forensischen Methoden oder auf KI-Methoden zur Verhinderung technischer Maßnahmen ermöglicht. Vor dem Hintergrund der aktuellen technischen Entwicklung ist dies dringend zu unterstützen.
- Um die Sicherheit und Effektivität solcher Methoden zu garantieren, sollte in der Begründung präzisiert werden, dass die entsprechenden Methoden mindestens das Schutzniveau „Stand der Technik“ vorweisen müssen und somit klargestellt ist, das die ausschließlich durch Menschen durchgeführte Verhinderung technischer Angriffe nicht ausreichend ist.

Zu §16:

- Der 2022 veröffentlichte Angriffsvektor auf Video-Ident-Verfahren zeigte maßgeblich eine Schwäche auf, die durch eine menschliche Prüfung kaum abwehrbar ist. Es sind dahingegen ausreichend sichere technische Verfahren bekannt, die die gezeigte „Präsentationsattacke“ aufdecken können.
- Die vorgesehene Teilautomatisierung nimmt jedoch keinen Bezug Maßnahmen zur Verhinderung technischer Angriffe. Nur die in § 9, §11 und §12 vorgesehenen Schritte sollen teilautomatisiert werden. Unklar bleibt, ob dabei §14 Anwendung in der Teilautomatisierung findet oder diese nur auf das klassische Video-Ident abzielt.
- Um eine hohe Sicherheit des Identifizierungsvorgangs zu garantieren, ist es deshalb notwendig, §16 insoweit zu ändern, dass §14 während der gesamten Teilautomatisierung Anwendung finden muss.
- Zudem gilt: Teilautomatisierte Lösungen wie in §16 vorgesehen, stellen zwar einen Gewinn für die Nutzererfahrung dar. Jedoch wird **durch eine menschliche Nachprüfung kein Sicherheitsvorteil geschaffen.**
- Verschiedene Untersuchungen zeigen, dass bspw. Grenzbeamte eine **Fehlerquote von bis zu 14% beim Abgleich von Gesichtern haben**[1]**.** Die hohe Fehlerquote bietet das Potential von Betrugsfällen und bleibt damit ein

[1] https://theconversation.com/passport-staff-miss-one-in-seven-fake-id-checks-30606; https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0103510.

Sicherheitsrisiko für den Finanzsektor, wenn die menschliche Prüfung genutzt werden muss[2].

- Zudem zeigen aktuelle Berichte zu Geldwäsche-Fällen in Post-Partnerfilialen, dass weiterhin große Gefahren von der Offline-Verifikation ausgehen[3].
- Wie im EU-Ausland bereits seit Jahren üblich, und im Sinne des Wettbewerbs auch dringend für deutsche Banken gewünscht, sollte die Teilautomatisierung zudem bedeuten, dass nicht nur die Prüfung der Ausweisdokumente teilautomatisiert stattfinden darf, sondern vor allem auch, **dass der gesamte Prozess ohne Live-Gespräch erfolgen kann. Der Einsatz technischer Maßnahmen anstelle eines Live-Gesprächs ist bereits seit vier Jahren im Rahmen des VDG und des TKG bewiesen.**
- Es gibt keine Studien oder Belege, dass Angriffe in etwa durch Social-Engineering oder Drucksituationen durch ein Live-Gespräch messbar abgewehrt werden können. Gleichwohl sind die Gefahren von Druck-Situationen und Social-Engineering durch eine fehlende Aufzeichnung des Verfahrens bei der eID gesteigert. Sollte also das Live-Gespräch als notwendige Maßnahme bei der Teilautomatisierung erwartet werden, **sollte dies bei der Nutzung der eID-Funktion ebenfalls gelten.**
- Es gilt daher sicherzustellen, dass die menschlichen Kontrollen konsequent durch technische Komponenten unterstützt oder überprüft werden, um **höchsten Sicherheitsstandards zu gewährleisten**.

Zu § 17:

- Vollautomatisierte Verfahren wie in §17 vorgesehen, können dahingehend einen **sichereren Umgang mit Identifizierungen gewährleisten**.
- Durch eine Sondergenehmigung des Bundesministeriums für Arbeit und Soziales wurden automatisierte Identifizierungsverfahren während der COVID-19-Pandemie bei der Bundesagentur für Arbeit bis August 2021 für die Onlinearbeitslosenmeldung eingesetzt. **Hier sind keine erfolgreichen Betrugsversuche bekannt.**
- Vollautomatisierte Identifizierungsverfahren wurden zudem zur Identifizierung im Rahmen der Hamburger Corona-Soforthilfen eingesetzt. **Auch hier konnte die Innovations- und Förderbank Hamburg alle Betrugsversuche erfolgreich durch das automatisierte Video-Ident aufklären und abwehren.**
- **Zudem wurde in beiden Fällen die herausragende Skalierbarkeit bei dauerhaft hohem Sicherheitsniveau bewiesen, während bei menschlich gestützten Verfahren die Qualität in stressigen Situationen leidet.**
- Wichtig ist daher mit Blick auf das Gefahrenpotenzial von Social Engineering und neuartigen technischen Möglichkeiten, eine **übergreifende Betrachtung der Gefahren und Bedrohungsszenarien**. Das hilft festzustellen, welche (technischen) Gegenmaßnahmen bei welchem Verfahren eine ausreichende

[2] bspw. wird im iProov im Threat Intelligence Report 2024 berichtet, dass Angreifer bewusst die menschliche Prüfung wählen: https://www.iproov.com/reports/iproov-threat-intelligence-report-2024;
[3] https://www.faz.net/aktuell/gesellschaft/kriminalitaet/kriminelle-sollen-post-partneragenturen-zur-geldwaesche-betrieben-haben-19701287.html

Sicherheit für die GwG-konforme Identitätsfeststellung gewährleisten, ohne einzelne Verfahren einseitig zu benachteiligen. Deshalb ist es wünschenswert, die angewandten Prüfverfahren **frühzeitig zu konkretisieren, für alle Verfahren (inkl. der eID) anzuwenden und jährlich zu wiederholen.**

- Vorstellbar ist eine Orientierung der Prüfkriterien an bestehenden Technischen Richtlinien, wie etwa der TR-03107 oder der TR-03147. So könnte dort, wo Vor-Ort-Kontrollen als Referenz gelten, festgelegt werden, **dass vollautomatisierte Verfahren das Sicherheitsniveau „substantiell“ der TR-03147 erreichen müssen.**

Die Nect GmbH ist einer der führenden Anbieter für digitale Identifizierungslösungen in Deutschland mit Sitz in Hamburg. Mit der Nect Wallet App bietet das Unternehmen u.a. ein automatisiertes Video-Ident, die eID, den ePass oder eine Wiederverwendungsfunktion. Außerdem sind qualifizierte elektronische Signaturen (QES) möglich. Die von Nect entwickelte Technologie wurde bereits von mehr als 10 Mio. Nutzern durchlaufen und kommt u.a. bei der R+V Versicherung, dem ADAC und der Telekom Deutschland zum Einsatz.

JUERGENS
Signed with my Nect Wallet
2024-05-16

Benny Bennet Jürgens

CEO und Gründer

bb@nect.com