kjm Kommission für Jugendmedienschutz

die medienanstalten

AG Technischer Jugendmedienschutz
Thema: Positivbewertung eines Altersverifikationssystems
Bearbeiter: (Landesanstalt für Medien NRW)
Düsseldorf, 28.04.2022

Beschlussvorlage für die 1. Sitzung der KJM (5. Amtsperiode) am 11.05. und 12.05.2022 in Halle (Saale)

TOP 18: Umsetzung der Anforderungen an ein Altersverifikationssystem (AVS) zur Sicherstellung einer geschlossenen Benutzergruppe nach § 4 Abs. 2 S. 2 JMStV: Bewertung des Konzepts „facial age estimation" der KYC AVC UK Ltd.

1 Beschlussempfehlung

Beschlussvorschlag:

a) Der Bericht AG „Technischer Jugendmedienschutz wird zustimmend zur Kenntnis genommen.

b) Die KJM stellt auf Grundlage der vorgelegten Unterlagen fest, dass das Konzept „facial age estimation" der KYC AVC UK Ltd. bei entsprechender Umsetzung und unter Berücksichtigung eines Puffers von 5 Jahren als nicht-änderbare Voreinstellung als Teillösung eines AVS i. S. d. § 4 Abs. 2 S. 2 JMStV auf der Stufe der Identifizierung geeignet ist.

Inhalte-Anbieter, die dieses Modul nutzen, müssen sicherstellen,

- dass nur bei der durch „facial age estimation" an ihn erfolgten Rückmeldung „identifiziert" ein Zugang zu Inhalten nach § 4 Abs. 2 S. 2 JMStV freigeschaltet wird (z. B. in Verbindung mit der persönlichen Auslieferung von Zugangsdaten per Einschreiben eigenhändig oder eine ähnlich qualifizierte Alternative im Sinne des AVS-Rasters der KJM) und

- dass die Weitergabe/Multiplikation der Zugangsdaten erschwert wird und dass zusätzliche Sicherungspflichten (wie z. B. Backdoorschutz, Time-Out nach bestimmter Idle-Time, zeitliche Begrenzung einer Sitzung) implementiert werden.

2 Bericht

2.1 Rechts- und Beschlusslage

Für die vorliegende Bewertung des Konzepts „facial age estimation" der KYC AVC UK Ltd. als geschlossene Benutzergruppe sind die entsprechenden Vorgaben gem. § 4 Abs. 2 S. 2 JMStV relevant:

Von Seiten des Anbieters ist für eine geschlossene Benutzergruppe sicherzustellen, dass bestimmte jugendgefährdende Angebote nur Erwachsenen zugänglich gemacht werden. Dies ist gemäß den Jugendschutzrichtlinien der Landesmedienanstalten grundsätzlich durch zwei Schritte sicherzustellen: durch eine Volljährigkeitsprüfung, die über persönlichen Kontakt erfolgen muss, und durch eine Authentifizierung beim einzelnen Nutzungsvorgang.

Eine Anerkennung von AV-Systemen durch die KJM ist im JMStV nicht vorgesehen. Die Verantwortung für die Sicherstellung einer geschlossenen Benutzergruppe liegt gemäß § 4 Abs. 2 S. 2 JMStV beim Anbieter. Aus Gründen der Rechts- und Planungssicherheit und zur besseren Durchsetzung wirksamer AV-Systeme bietet die KJM interessierten Anbietern und Unternehmen jedoch an, ihre Konzepte und Module zur Sicherstellung geschlossener Benutzergruppen daraufhin zu überprüfen, ob sie den gesetzlichen Anforderungen genügen, und für diesen Fall eine positive Bewertung zu erteilen.

Die KJM bewertet Konzepte für Gesamt- und Teillösungen (Module) für geschlossene Benutzergruppen. Module können etwa Verfahren nur für die Identifizierung oder nur die Authentifizierung oder andere wesentliche Bestandteile eines AV-Systems sein. Die Bewertung von Modulen ermöglicht Anbietern eine leichtere Umsetzung in der Praxis. So besteht für Anbieter die Möglichkeit, positiv bewertete Module im Baukastenprinzip zu Gesamtlösungen von AV-Systemen zu kombinieren, die dann den Anforderungen des JMStV und der KJM entsprechen.

Die Bewertung der vorgelegten Konzepte im Einzelfall erfolgt dabei auf der Grundlage eines von der AG Technischer Jugendmedienschutz erarbeiteten und von der KJM beschlossenen Kriterienrasters, welches die in § 4 Abs. 2 S. 2 JMStV und in den Jugendschutzrichtlinien der Landesmedienanstalten getroffenen Vorgaben weiter konkretisiert und ausdifferenziert. Die KJM hat zuletzt in ihrer Sitzung am 11. Dezember 2019 eine überarbeitete Version („AVS-Raster" gültig seit dem 11.12.2019, vgl. Anlage 1) des Bewertungsrasters beschlossen, die nun maßgebend für die Bewertung des Konzepts „facial age estimation" heranzuziehen ist.

Im Bereich der Konzepte zur Sicherstellung von geschlossenen Benutzergruppen nach § 4 Abs. 2 S. 2 JMStV ist kein offizielles Anerkennungsverfahren geregelt, die KJM bietet aber interessierten Anbietern ihr Verfahren der Positivbewertung an.

2.2 Sachstand zu „facial age estimation"
Mit E-Mail vom 22.03.2022 beantragte die KYC AVC UK Ltd. eine Positivbewertung des Systems „facial age estimation" als Konzept einer geschlossenen Benutzergruppe. Beigefügt war eine Beschreibung des Konzepts (vgl. Anlage 2).

Die AG Technischer Jugendmedienschutz hat die zur Bewertung vorgelegten Unterlagen in einer Videokonferenz geprüft und abschließend bewertet.

3 Beschreibung des Konzepts „facial age estimation"

Bei „facial age estimation" handelt es sich um ein Tool zur Alterseinschätzung mittels künstlicher Intelligenz. Inhalteanbieter können dieses Tool in ihren eigenen Telemedienangeboten implementieren, um so das Alter von Nutzern einschätzen zu können.

Die dahinterstehende Technik besteht aus einem neuronalen Netzwerk, welches mittels einer Vielzahl von Gesichtsbildern dazu trainiert wurde, das Alter anhand biometrischer Daten einzuschätzen.

Zur Alterseinschätzung hat der Nutzer in die Kamera des Telefons oder in die Webcam des Computers zu schauen. Das Bild wird sodann erfasst und an den Server der KYC AVC UK Ltd. übertragen. Mittels des neuronalen Netzwerks wird das Alter anhand des Bildes eingeschätzt. Ein Download einer App oder die Einreichung von Ausweisdokumenten werden für die Alterseinschätzung nicht benötigt.

. Der Nutzer erhält im Anschluss Zugang zu den jeweiligen Inhalten.

„facial age estimation" hält Vorkehrungen bereit, die Manipulationen bei der Altersermittlung verhindern solle. Das Verfahren zur Ermittlung von Gesichtern erkennt, ob es sich bei der Live-Aufnahme um eine reale, lebendige Person handelt (Lebenderkennung) oder ob versucht wird, das System durch Nutzung einer Fotografie oder eines Videos von einer anderen, älteren Person zu täuschen. Bei Feststellung eines möglichen Manipulationsversuchs bricht die Altersermittlung ab.

Im Übrigen wird auf die von der der KYC AVC UK Ltd. eingereichten Unterlagen verwiesen.

4 Bewertung des Systems „facial age estimation"

Bei der Prüfung des Systems „facial age estimation" der KYC AVC UK Ltd. kam die AG Technischer Jugendmedienschutz der KJM auf Basis des vorgelegten Konzepts mehrheitlich zu dem Ergebnis, dass dieses – unter Zugrundelegung der im AVS-Raster der KJM niedergelegten Bewertungskriterien (gültig seit dem 11.12.2019) und dem Änderungsvorschlag der AG „Technischer Jugendmedienschutz" – in der vorgelegten Version und bei entsprechender Umsetzung als Modul auf

der Stufe der Identifizierung im Sinne der KJM-Kriterien zur Sicherstellung einer geschlossenen Benutzergruppe für Erwachsene gem. § 4 Abs. 2 S. 2 JMStV geeignet ist.

Bei dem System „facial age estimation" handelt es sich um ein Identifizierungskonzept, welches eine Identifizierung mittels eines automatisierten Prozesses unter Abgleich biometrischer Daten ermöglicht.

Gemäß des „AVS-Rasters" der KJM (gültig seit dem 11.12.2019) muss zumindest die einmalige Identifizierung von Interessenten für eine geschlossene Benutzergruppe grundsätzlich durch persönlichen Kontakt erfolgen. Unter „persönlichem Kontakt" ist grundsätzlich eine Angesichts-Kontrolle unter Anwesenden („face-to-face"-Kontrolle) mit Vergleich von amtlichen Ausweisdaten (Personalausweis, Reisepass) zu verstehen.

Von einer Angesichts-Kontrolle unter Anwesenden („face-to-face"-Kontrolle) kann abgesehen werden, wenn die Identifizierung mittels einer Software durch einen Vergleich der biometrischen Daten des Ausweisdokuments und einem Lichtbild des zu Identifizierenden sowie einer automatischen Erfassung der Daten des Ausweisdokuments erfolgt.

Nach dem Änderungsvorschlag der AG „Technischer Jugendmedienschutz" im Hinblick auf das AVS-Raster kann von einer Angesichts-Kontrolle unter Anwesenden („face-to-face"-Kontrolle) mit Vergleich von amtlichen Ausweisdaten (Personalausweis, Reisepass) abgesehen werden, wenn für die Altersprüfung ein Verfahren auf Grundlage einer automatisierten kamerabasierten Altersermittlung genutzt wird, in dessen Rahmen eine Software Aussagen über die Wahrscheinlichkeit des Alters der zu identifizierenden Person anhand eine eines Live-Kamerabildes trifft.

Im Hinblick auf das von BVerwG und BGH entwickelte Konzept der „effektiven Barriere", welches vorsieht, dass „wirksame Vorkehrungen" auch von den Anbietern relativ unzulässiger Angebote nach § 4 Abs. 2 JMStV gewährleistet werden müssen (BVerwGE 116, 5, 14 f.; BGH NJW 2008, 1882, 1884), erfüllte „facial age estimation" die Anforderungen an eine solche effektive Barriere.

Nach der Rechtsprechung ist die Wirksamkeit dort erreicht, wo einfache, naheliegende und offensichtliche Umgehungsmöglichkeiten ausgeschlossen sind. Dabei sind solche Fälle und Umstände nicht zu beachten, in denen Jugendliche auf Basis kaum vorhersehbarer besonderer Kenntnisse, Fertigkeiten oder Anstrengungen ausnahmsweise die Überprüfung umgehen. Laut Rechtsprechung des BGH sind ausdrücklich auch rein technische Altersverifikationsformen möglich, „wenn sie den Zuverlässigkeitsgrad einer persönlichen Altersprüfung erreichen" (BGH NJW 2008, 1882, 1885).

Die zentrale Frage für die Beurteilung eines Altersverifikationssystems ist damit die Verlässlichkeit des Altersüberprüfungsverfahrens, auch – aber nicht ausschließlich – im Vergleich mit Formen der persönlichen Altersüberprüfung.

Entscheidend für Aussagen über die Plausibilität der Altersermittlung sind zum einen die ermittelten sogenannten mittleren absoluten Fehler (mean absolute errors, MAE), d. h. die Höhe der Abweichungen der Altersschätzung vom tatsächlichen Alter einer Person. Im Bereich der Altersverifikation sind zum anderen die sog. „false positives"-Raten (Falsch-positiv-Raten oder Falscherkennungsraten) relevant, d. h. der Prozentsatz derjenigen Fälle, in denen die Software denjenigen Nutzenden, die das jugendschutzrechtlich relevante Grenzalter eigentlich noch nicht erreicht haben, ein höheres Alter attestiert und entsprechend den Zugang zu jugendschutzrelevanten Inhalten ermöglichen würde. Der umgekehrte Fall, d. h. die Software ermittelt bei einer Person, die die Altersgrenze schon erreicht hat, ein zu junges Alter (sog. „false negative" oder Nichterkennung), ist für eine jugendschutzrechtliche Beurteilung der Plausibilität grundsätzlich unschädlich.

Mit Blick auf die Zuverlässigkeit der richtigen Alterseinschätzung ist zu berücksichtigen, dass es auch bei einem automatisierten System nicht ausgeschlossen ist, dass zu junge Nutzer*innen als bereits volljährig eingeschätzt werden. Aus dem Antrag ergibt sich, dass statistisch

Durch die Erhöhung des Alterspuffers (sog. threshold) kann die Prozentzahl der relevanten falsch-positiven Alterseinschätzungen verringert werden. Ein erhöhter Puffer fungiert also bei altersmäßigen Grenzfällen wie ein Zweifel bei menschlichen Altersüberprüfungen. Die Fehlerkennungsrate von „facial age estimation" liegt bei einem Alterspuffer von drei Jahren (d. h. das Grenzalter liegt dann bei 21 Jahren) bei nur noch Prozent und bei einem Alterspuffer von 5 Jahren (d. h. das Grenzalter liegt dann bei 23 Jahren) bei nur noch Prozent) bzw. Prozent der Alterseinschätzungen von Minderjährigen durch „facial age estimation" sind dann aus Sicht des Jugendmedienschutzes korrekt. Aus Sicht der Mehrheit der AG „Technischer Jugendmedienschutz" ist für die KYC AVC UK Ltd. davon auszugehen, dass mit einem Puffer von 5 Jahren ein mindestens vergleichbares Schutzniveau wie bei einer menschlichen Alterserkennung gewährleistet werden kann. Dieser Wert entspricht jedenfalls mindestens der geforderten „hohen Wahrscheinlichkeit" der Feststellung der Volljährigkeit.

4.1 Zusätzliche Pflichten des Telemedien-Anbieters, der „facial age estimation" als AVS-Teilmodul einsetzt

Bei dem Konzept „facial age estimation" der KYC AVC UK Ltd. handelt es sich um eine Teillösung und damit um ein Modul auf der Stufe der

Identifizierung, das z. B. von einem Inhalte- oder anderen AVS-Anbieter im Baukastenprinzip als Bestandteil einer AVS-Gesamtlösung eingesetzt werden kann. Es obliegt dem Telemedien-Anbieter/Inhalte-Anbieter, selbst mit weiteren Maßnahmen sicherzustellen, dass nur nach einer durch „facial age estimation" an ihn erfolgten Rückmeldung „identifiziert" ein Zugang zu Inhalten nach § 4 Abs. 2 S. 2 JMStV freigeschaltet wird. Der Content-Anbieter oder AVS-Betreiber kann den Identifizierungsprozess z. B. dadurch abschließen, dass er die Zugangsdaten im persönlichen Kontakt an die als volljährig bestätigte Person unter den Adressdaten aushändigen lässt, die mit „facial age estimation" verifiziert wurden (z. B. Einschreiben eigenhändig oder eine ähnlich qualifizierte Alternative, die sicherstellt, dass nur die als volljährig identifizierte Person die Zugangsdaten bzw. eine Zugangsberechtigung erhält (zu den näheren Voraussetzungen vgl. das „AVS-Raster" der KJM in Anlage 1).

Zudem obliegt dem Telemedien-Anbieter/Inhalte-Anbieter, selbst mit weiteren Maßnahmen sicherzustellen, dass im Rahmen der Authentifizierung nur die jeweils identifizierte und altersgeprüfte Person Zugang zur geschlossenen Benutzergruppe erhält und die Weitergabe der Zugangsberechtigung an unautorisierte Dritte erschwert wird. Dabei sind ausreichende Schutzmaßnahmen zur Erschwerung der Multiplikation und der Nutzung von Zugangsberechtigungen durch unautorisierte Dritte zu ergreifen. Der Weitergabeschutz kann dabei entweder durch technische Maßnahmen zur Erschwerung der Multiplikation oder durch persönliche Risiken in der Sphäre des Nutzers realisiert werden (zu den näheren Voraussetzungen vgl. das „AVS-Raster" der KJM in Anlage 1).

Unberührt bleiben darüber hinaus zusätzliche Sicherungspflichten, die durch den Telemedien-Anbieter/Inhalte-Anbieter beim jeweiligen Nutzungsvorgang zu gewährleisten sind, wie z. B. Backdoorschutz, Time-Out nach bestimmter Idle-Time, zeitliche Begrenzung einer Sitzung usw.

4.2 Minderheit innerhalb der AG „Technischer Jugendmedienschutz"
Die Minderheit innerhalb der AG „Technischer Jugendmedienschutz" ist hingegen der Auffassung, dass „facial age estimation" die gesetzlichen Anforderungen des § 4 Abs. 2 S. 2 JMStV im Hinblick auf die Identifizierung nicht erfüllt. Sie geht davon aus, dass die Technologie der „Age Estimation" mittels künstlicher Intelligenz für Deutschland noch nicht ausgereift und somit nicht marktreif ist. Sie befürchtet weiter, dass diese unreife Version zu einem massiven Overblocking führen werde.

5 Ergebnis

Die AG Technischer Jugendmedienschutz kam mehrheitlich zu dem Ergebnis, dass das Konzept „facial age estimation" der KYC AVC UK Ltd. bei entsprechender Umsetzung und unter Berücksichtigung eines Puffers von 5 Jahren als nicht-änderbare Voreinstellung die gesetzlichen Anforderungen des § 4 Abs. 2 S. 2 JMStV im Hinblick auf die

Identifizierung erfüllt, sofern der Inhalteanbieter mit zusätzlichen Mitteln sicherstellt, dass nur bei als volljährig identifizierten Nutzern nach Zustellung von Zugangsdaten ein Zugang zu Inhalten nach § 4 Abs. 2 S. 2 JMStV freigeschaltet wird und er zusätzliche Sicherungspflichten implementiert (wie z. B. Maßnahmen zur Erschwerung der Multiplikation/Weitergabe der Zugangsdaten, Backdoorschutz, Time-Out nach bestimmter Idle-time, zeitliche Begrenzung einer Sitzung).

verifymyage

18 & 18+ – Facial Age Estimation

ISSUED BY

VerifyMyAge. *This is an **extremely sensitive** document, **NOT** to be shared any wider than is necessary for approval.*

REPRESENTATIVE

Head of Customer Success

26 April 2022

V1.3

Facial Age Estimation Check

An attempt to verify the user's age, via a Facial Age Estimation check is performed.

Part 1: Liveness & Anti-Spoofing Checks

- The user first provides a 3D FaceScan using a selfie video taken on any camera-enabled device.
    - This is used to determine "Liveness", that is, determining that we are interfacing with a physically present human being, and not an inanimate spoof artefact or injected video/data *(supplier - FaceTec)*.
- We protect against Level 1-5 Threat Vectors
    - **Level 1 (A)** - Hi-res paper & digital photos, hi-def challenge/response videos and paper masks.
    - **Level 2 (B)** - Commercially available lifelike dolls, and human-worn resin, latex & silicone 3D masks under $300 in price.
    - **Level 3 (C)** - Custom-made ultra-realistic 3D masks, wax heads, etc., up to $3,000 in creation cost.
    - **Level 4** -Decrypt & edit the contents of a 3D FaceMap™ to contain synthetic data not collected from the session, have the Server process and respond with Liveness Success.
    - **Level 5** - Take over the camera feed & inject previously captured video frames or a deepfake puppet that results in the FaceTec AI responding with "Liveness Success."
- If Liveness cannot be successfully determined, the user is asked to try again.
    - Once all available attempts have been unsuccessful, the verification fails.
- If Liveness is successfully determined we move to Part 2.

Part 2: Age Estimation

- If the Liveness Check is successful a 2D image of the user, which is captured during the selfie video, is then submitted to our AI for Age Estimation

- A Yes/No result is then returned to the business as to whether or not the user has passed based on a pre-set threshold.
    - If the user's age cannot be successfully determined, the user is asked to try again.

- Once all available attempts have been unsuccessful, the verification fails.

Facial Age Estimation Accuracy

- Our Facial Age Estimation system has an equally weighted MAE of overall. However, the important age groups (related to sectors with well-established age-restricted legislation e.g. alcohol, tobacco and pornography, and newly-emerging age-restricted legislation e.g. social media and online video gaming) have the lowest MAE at
  meaning they are more accurately predicted.

GEN I			
AGE	MALE	FEMALE	ALL
TOTAL			

- Our Facial Age Estimation system also contains no observable bias across the six skin tones of the Fitzpatrick Scale.
  - The Fitzpatrick Scale uses six bands, from Type I (lightest) to Type VI (darkest) and, for the purposes of this document, data is presented in three segments (Types I and II, Types III and IV and Types V and VI).
    - Our test data set was tagged manually, with quality control measures in place to ensure the process was robust and free from human bias.

GEN I				
AGE	SKIN TONE TYPE I & II	SKIN TONE TYPE III & IV	SKIN TONE TYPE V & VI	ALL
TOTAL				

- As described above (Facial Age Estimation Accuracy) our Facial Age Estimation system has a margin of error which can produce results which are known as false positives.
    - A false positive occurs when our solution estimates that an individual is above a stated age of interest but, in fact, they are not.
        - For this reason industry best practice dictates that a safety buffer is used to reduce or eliminate these results.
            - The table below demonstrates false-positive rates across 14 - 17-year-olds, for a succession of age thresholds:

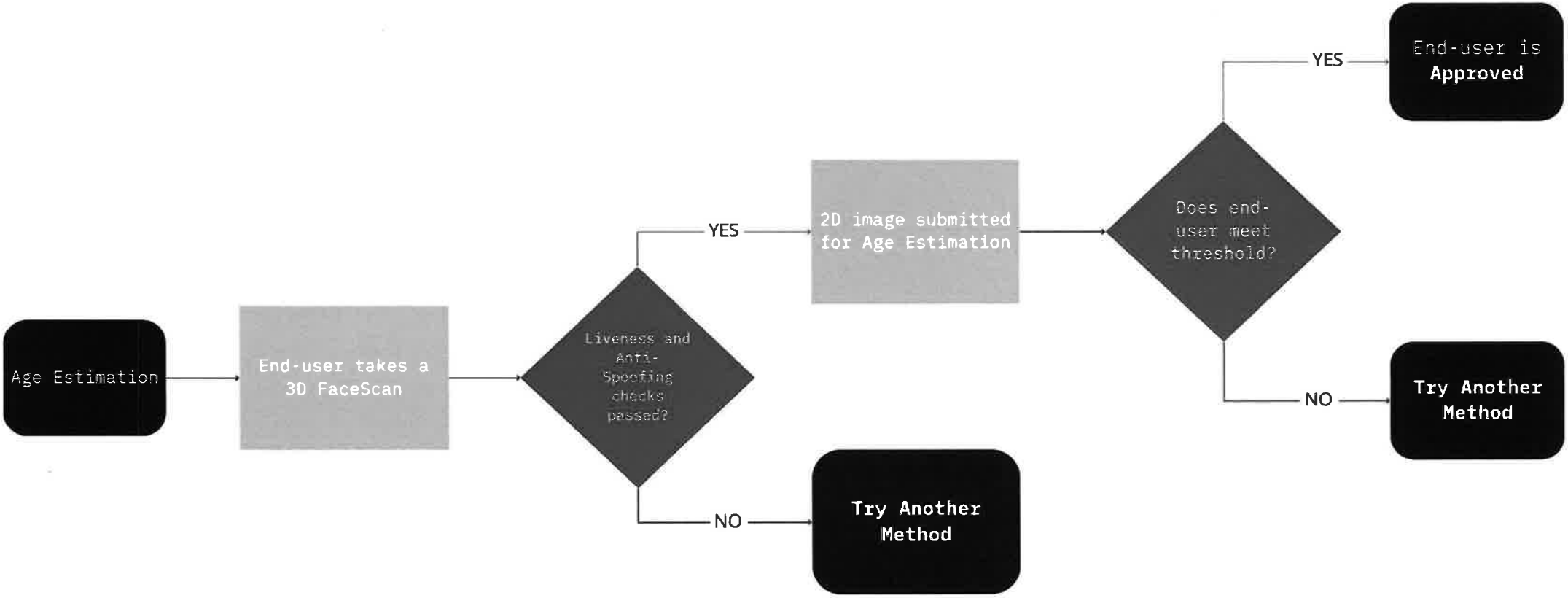
Threshold (years)	AGE (SAMPLE SIZE)				Average False Positive Rate (weighted equally for each age)
	14 (4,200)	15 (4,773)	16 (5,991)	17 (7,220)	
20					
21					
22					
23					
24					
25					
26					
27					
28					
29					
30					

Appendix

2. FaceTec Liveness Certifications for Level 1 – 5 Threat Vectors

*There are no NIST/NLVAP lab tests available for PAD Level 3, or Levels 4 & 5 bypasses, as those attack vectors are missing from the ISO 30107-3 standard and thus all associated lab testing. Only a Spoof Bounty Program can currently address Levels 1-5.

3. Facial Age Estimation Accuracy


Age Estimation
End-user takes a 3D FaceScan
Liveness and Anti-Spoofing checks passed?
YES
NO
Try Another Method
2D image submitted for Age Estimation
Does end-user meet threshold?
YES
End-user is Approved
NO
Try Another Method

verifymyage

KYC AVC UK LTD trades under the brands VerifyMyAge & VerifyMyContent

Practice Statement

KYC AVC UK LTD is a data-driven, innovative age verification company. Our mission is to provide a safe and frictionless online Age Verification solution that successfully verifies 100% of our customers' legitimate end-users. Through a combination of best-in-class technology and a deep understanding of our customers' requirements, our proven Age Verification solution is the most advanced product on the market.

How it works:

Please note:

- *Suppliers of* KYC AVC UK LTD *are indicated in (brackets).*
- *ALL data is kept within the EU & we meet all relevant storage and transfer requirements.*
- *No personal data is stored on minors i.e. those under 18.*
- *For the purpose of this document a 'Customer' is our client (B2B) & an 'end-user' is our client's customer whose age we are verifying (B2C)*

Overview of applicable products/content, age restrictions & re-authentication requirements

Rating	Definition	Reauthentication
18+	online content/services, e-commerce with goods rated 18+ (e.g. pornography)	reauthentication to access online content/services

verifymyage

18+ - online content/services, e-commerce with goods rated 18+ (e.g. pornography)

Automated age verification process

Upon a Customer's receipt of a request from an end-user to access '18+' rated content or products (e.g. pornography), the following steps occur:

If available, one, some or all of the end-users name, address, email, username, date of birth (DOB) and mobile telephone number are passed to KYC AVC UK LTD from the Customer's database via an API as part of our *automatic* age-verification process.

- An attempt to verify the end-users age, via the submitted name, address and DOB is performed through a Credit Reference Bureau *(Schufa)*. This involves confirming the presence of the end-users details with *(Schufa)* on their *IdentCheck Premium* database; the presence of the end-users name, address and DOB on this version of their database confirms the end-user is at least 18 years old and that a valid government-issued identity document for this end-user has been seen and authenticated.
    -
    -

- If a negative value is returned or the above information is not available because the Customer has not previously collected this from the end-user (e.g. Adult website), the end-user is notified via email or directly in the browser that the *automatic* age-verification process was unable to be completed by KYC AVC UK LTD and asks them to verify themselves via our web application either directly in the browser or via a link using one of the following options:

The following options are presented to the user simultaneously via our web-app, for them to choose the most appropriate option.

1. ID Scan with 3D Face Match & Liveness Detection

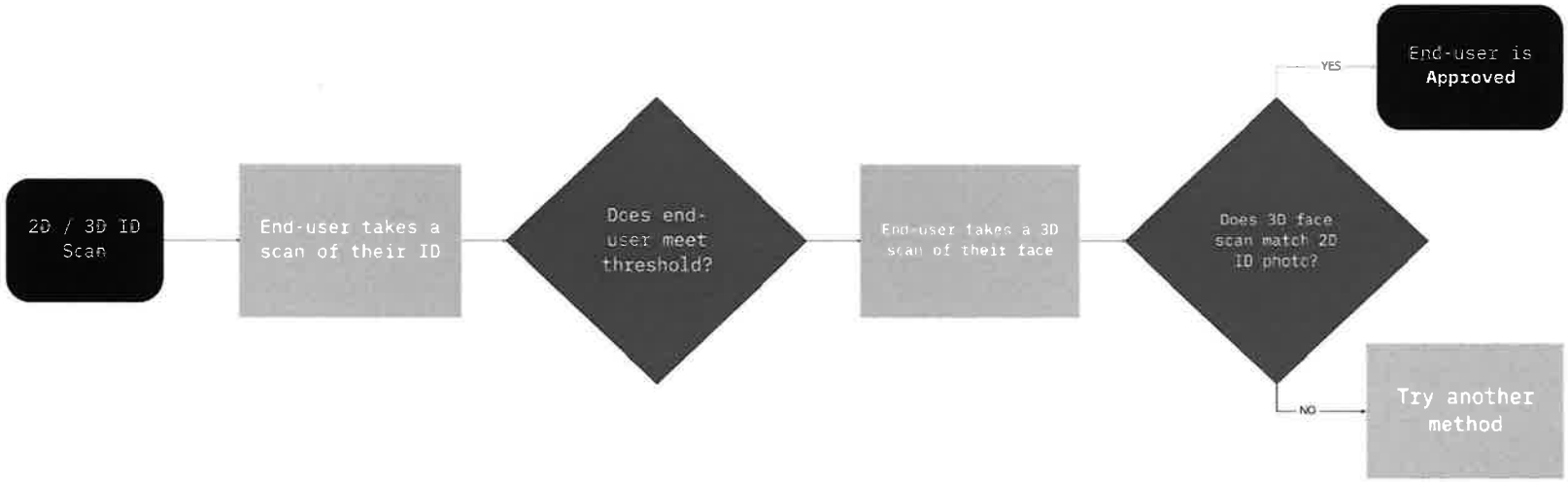
- An attempt to verify the end-users age, via a government-issued ID scan performed. The end-user provides a scan of a government-issued ID using a camera-enabled device, into the KYC AVC UK LTD web app.
- This image is submitted to KYC AVC UK LTD and processed with third-party software to extract data from of the identity document. The data is then "triangulated" with three points of assuredness;
    -
    -
    -
- If available, Knowledge Point 1 is checked against the same field in the order placed by the end-user. Knowledge Point 2 is checked for a valid format, according to the relevant fields in the document. Possession results include performing Digital ID Anti-Spoof checks and ID Photo Anti-Tamper checks by specialist software If a positive result is returned for all three points, the end-user is notified within the web app that their ID scan was successful.

- If Knowledge Point 1 is not available, and a positive result is returned for Knowledge Point 2 and Possession the end-user is notified within the web app that their ID scan was successful.

- A 2D to 3D face match is then performed to ensure the person presenting the document at this moment in time is the document owner.

Rules for 2D to 3D Face Match

- The end-user first provides a 3D FaceScan using a selfie video taken on any camera-enabled device.
  - This is used to determine "Liveness", that is, determining that we are interfacing with a physically present human being, and not an inanimate spoof artefact or injected video/data *(Supplier - FaceTec)*.
- FaceTec protects against Level 1-5 Threat Vectors -
  - **FaceTec Liveness Certifications**
    -
    -
    -
      - *There are no NIST/NLVAP lab tests available for PAD Level 3, or Levels 4 & 5 bypasses, as those attack vectors are missing from the ISO 30107-3 standard and thus all associated lab testing. Only a Spoof Bounty Program can currently address Levels 1-5.
- If Liveness cannot be successfully determined, the user is asked to try again.
  - Once all available attempts have been unsuccessful, the verification fails.
- The Photo ID Match process only succeeds if the end-user passes Liveness and the Live end-user matches the face present on the government issued Photo ID (FaceTec).



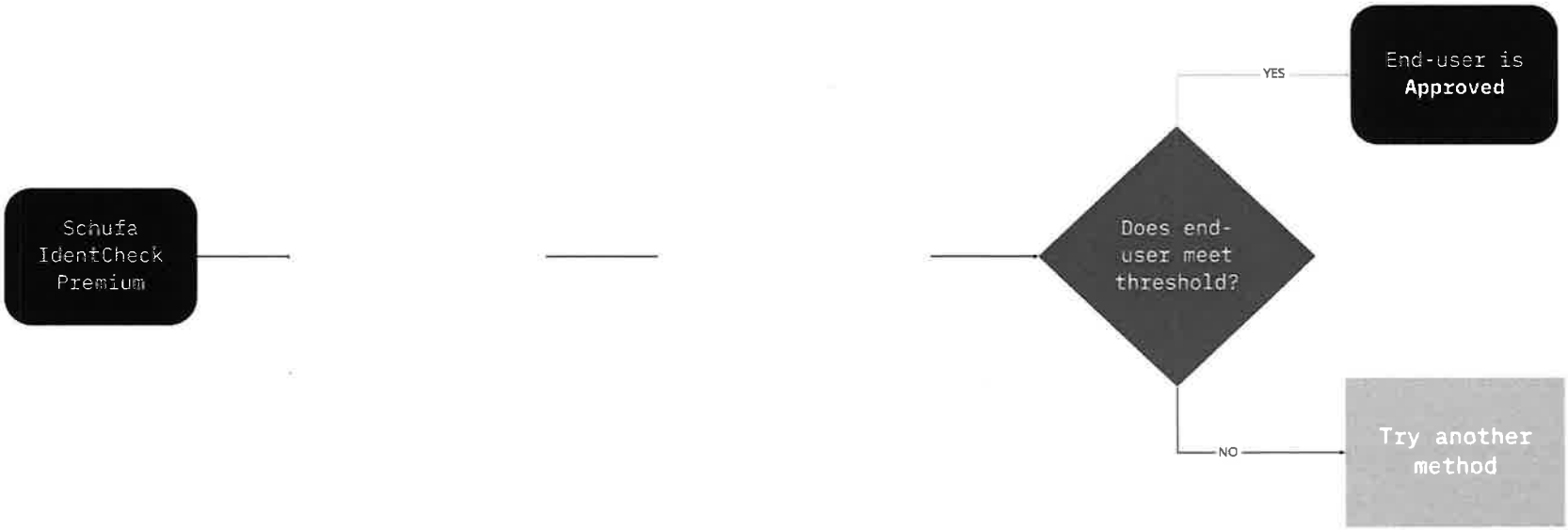
2. Open Banking via yes.com

- An attempt to verify the end-users age via their Volksbanken Raiffeisenbanken or Sparkassen bank account is performed by integrating directly with yes.com and using their technology, which is a KJM-approved age verification system.

3. Schufa IdentCheck Premium + Open Banking

If an end-user holds a bank account that is not Volksbanken Raiffeisenbanken or Sparkassen, then an attempt to verify the end-users age can be performed via a combination of open banking under the Payment Services Directive 2 (PSD2) and the *Schufa Identcheck Premium* service.

-
  -
    -
    -
-
  -
-
  -
-
  -



NB. The end-user is given 3 attempts to verify via each option, after the 3rd attempt they are invited to try another method. If all methods have been attempted, a negative result is returned and the end-user is notified they have failed the age-verification process.

4. Credit Card with 3D Secure

An attempt to verify the end-users age, via a Credit Card check combined with 3DSecure is performed via our Payment Processor

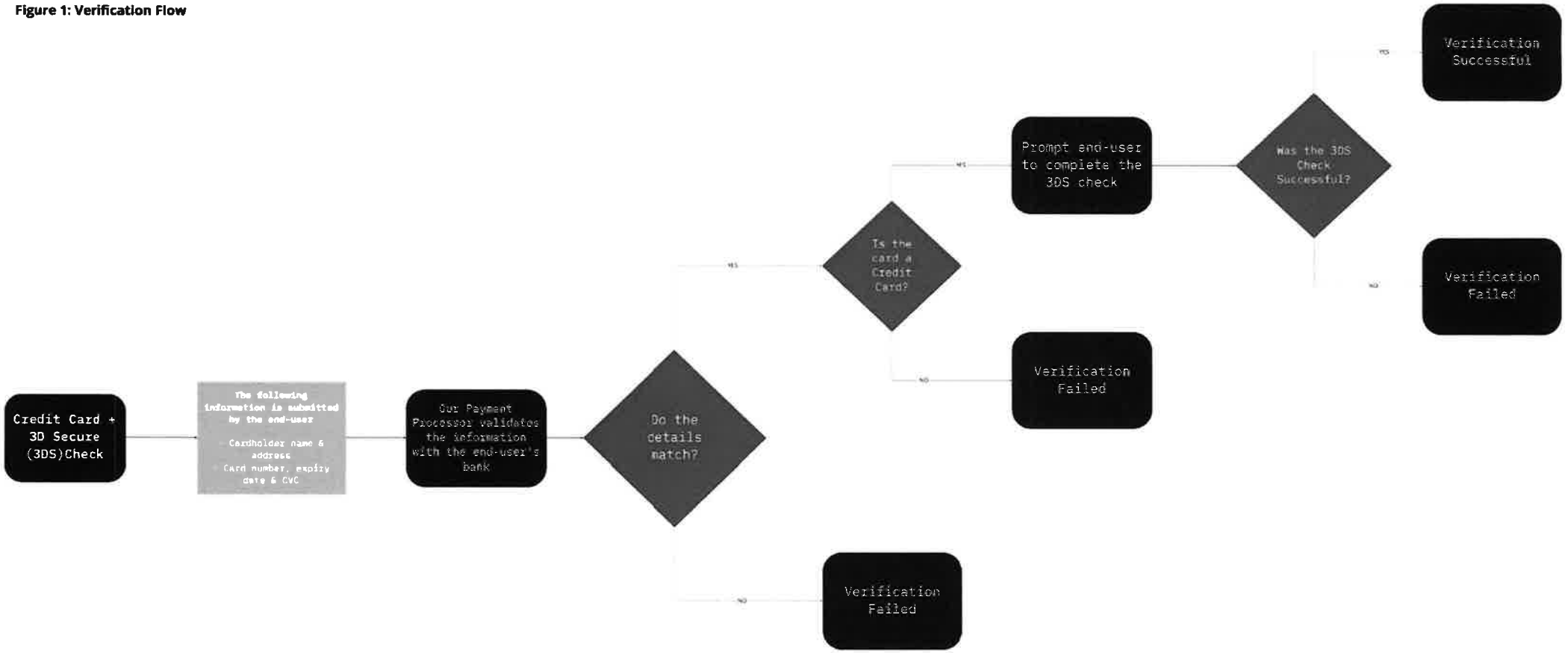
- The end-user is asked to enter the following information via an iFrame in our web application which provides the highest level of security & ensures compliance with Payment Card Industry standards (PCI Security Standards Council), protecting the end-users data;
    - cardholder name & address
    - card number, expiry date & CVC (3 digit security code on the card)
- A check is then performed by our payment processor to ensure all of the data which is entered by the end-user matches the data which their bank holds for them.
    - If any of the checks fail, the end-user fails verification.
    - If all checks pass a further check is carried out on the card number as described below:
-
    -

- [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
- Once we have then determined the card is a "true" 'credit' card and therefore that the holder must be over 18, the 3DSecure process is triggered to confirm the person who has entered the card details is the account holder;
  - The user will be redirected to their bank to login and complete the authentication process where they will be asked for 2 out of 3 pieces of information below;
    - something the user is, for example their fingerprint
    - something the user has, for example their phone
    - something the user knows, for example a password
- Once the user passes the 3DSecure check they are successfully verified, if they fail the 3DSecure check they will be asked to verify their age via another approved method.

NB. The end-user is given 3 attempts to verify via each option, after the 3rd attempt they are invited to try another method. If all methods have been attempted, a negative result is returned and the end-user is notified they have failed the age-verification process.

verifymyage

Figure 1: Verification Flow



5. Facial Age Estimation

An attempt to verify the user's age, via a Facial Age Estimation check is performed.

Part 1: Liveness & Anti-Spoofing Checks

- The user first provides a 3D FaceScan using a selfie video taken on any camera-enabled device.
    - This is used to determine "Liveness", that is, determining that we are interfacing with a physically present human being, and not an inanimate spoof artefact or injected video/data *(supplier - FaceTec)*.
- We protect against Level 1-5 Threat Vectors
    - **Level 1 (A)** - Hi-res paper & digital photos, hi-def challenge/response videos and paper masks.
    - **Level 2 (B)** - Commercially available lifelike dolls, and human-worn resin, latex & silicone 3D masks under $300 in price.
    - **Level 3 (C)** - Custom-made ultra-realistic 3D masks, wax heads, etc., up to $3,000 in creation cost.
    - **Level 4** -Decrypt & edit the contents of a 3D FaceMap™ to contain synthetic data not collected from the session, have the Server process and respond with Liveness Success.
    - **Level 5** - Take over the camera feed & inject previously captured video frames or a deepfake puppet that results in the FaceTec AI responding with "Liveness Success."
- If Liveness cannot be successfully determined, the user is asked to try again.
    - Once all available attempts have been unsuccessful, the verification fails.
- If Liveness is successfully determined we move to Part 2.

verifymyage

Part 2: Age Estimation

- If the Liveness Check is successful a 2D image of the user, which is captured during the selfie video, is then submitted to our AI for Age Estimation

- A Yes/No result is then returned to the business as to whether or not the user has passed based on a pre-set threshold.
    - If the user's age cannot be successfully determined, the user is asked to try again.
        - Once all available attempts have been unsuccessful, the verification fails.

Facial Age Estimation Accuracy

- Our Facial Age Estimation system has an equally weighted MAE of 2.93 overall. However, the important age groups (related to sectors with well-established age-restricted legislation e.g. alcohol, tobacco and pornography, and newly-emerging age-restricted legislation e.g. social media and online video gaming) have the lowest MAE at , meaning they are more accurately predicted.

GEN I			
AGE	MALE	FEMALE	ALL
TOTAL			

- Our Facial Age Estimation system also contains no observable bias across the six skin tones of the Fitzpatrick Scale.
    - The Fitzpatrick Scale uses six bands, from Type 1 (lightest) to Type VI (darkest) and, for the purposes of this document, data is presented in three segments (Types I and II, Types III and IV and Types V and VI).
        - Our test data set was tagged manually, with quality control measures in place to ensure the process was robust and free from human bias.

GEN I				
AGE	SKIN TONE TYPE I & II	SKIN TONE TYPE III & IV	SKIN TONE TYPE V & VI	ALL
TOTAL				

- As described above (Facial Age Estimation Accuracy) our Facial Age Estimation system has a margin of error which can produce results which are known as false positives.
    - A false positive occurs when our solution estimates that an individual is above a stated age of interest but, in fact, they are not.
        - For this reason industry best practice dictates that a safety buffer is used to reduce or eliminate these results.
            - The table below demonstrates false-positive rates across 14 - 17-year-olds, for a succession of age thresholds:

Threshold (years)	AGE (SAMPLE SIZE) 14	15	16	17	Average False Positive Rate (weighted equally for each age)
20					
21					
22					
23					
24					
25					
26					
27					
28					
29					
30					

verifymyage

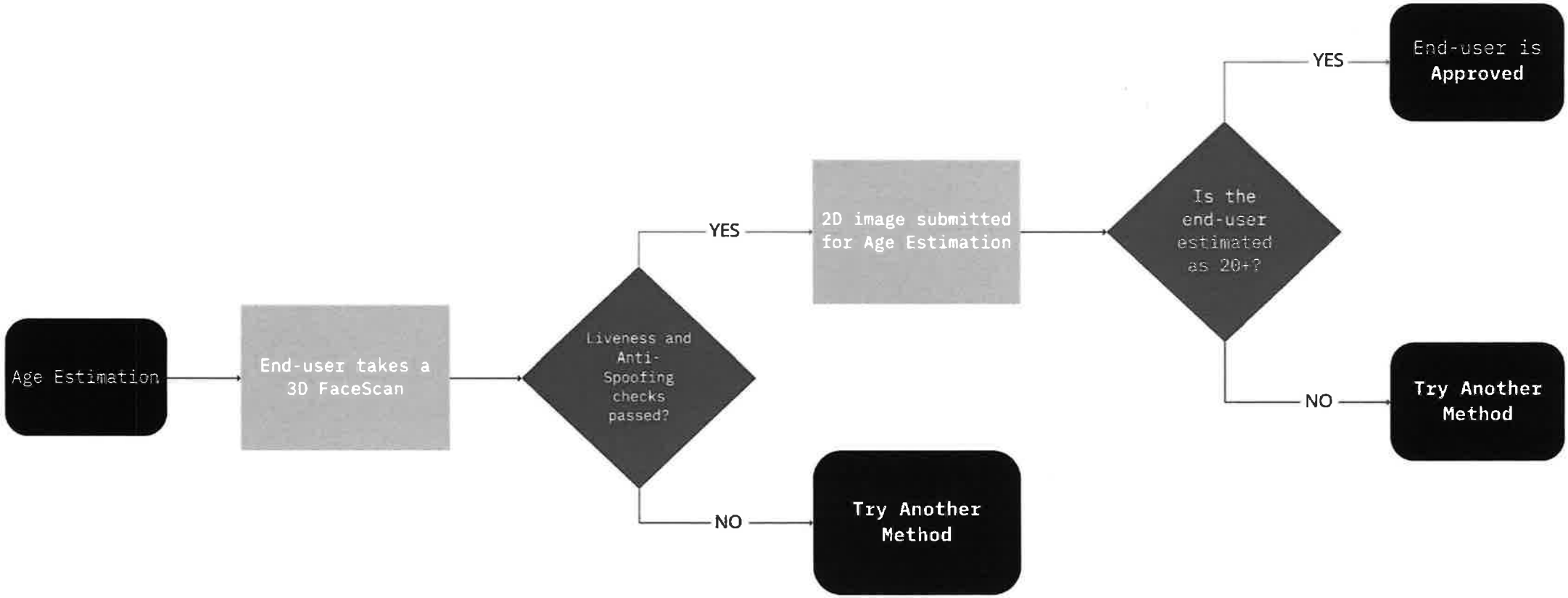
Appendix

2. **FaceTec Liveness Certifications for Level 1 - 5 Threat Vectors**
    -
    -
    -

*There are no NIST/NLVAP lab tests available for PAD Level 3, or Levels 4 & 5 bypasses, as those attack vectors are missing from the ISO 30107-3 standard and thus all associated lab testing. Only a Spoof Bounty Program can currently address Levels 1-5.

3. **Facial Age Estimation Accuracy**

verifymyage



Reauthentication

- Once an end-user has verified their age they will be asked to take a quick video selfie which will act as their password to reauthenticate when they attempt to access age-restricted content or products in the future.
    - If the Facial Biometrics option isn't available we will use their mobile phone number to send a one-time passcode (OTP).
- Once VerifyMyAge recognises a returning user they will be asked to reauthenticate themselves via one of the above methods.
    - This prevents unauthorised access on a verified device or account by a minor.

verifymyage

Monitoring and Certifications (UK & DE)

KYC AVC UK Ltd is certified under PAS1296:2018 (UK).

KYC AVC UK LTD has been subject to conformity assessment in accordance with the Publicly Available Specification (PAS) 1296:2018 Code of Practice for Online Age Verification and validated by the Age Check Certification Scheme.
Certificate

The audit process for PAS 1296:2018 is split into three parts:

- Policy Evaluation - An evaluation of our age check policies was achieved by building a detailed understanding of our approach to age checks, our practice statements, our approach to data privacy, protection and security, our approach to age validation, our commercial model(s) and our management of age attributes. The policy evaluation explores the approach we take to the provision of age check services and the decisions we make on the application of our age check policies and procedures.
- Quality Evaluation - Auditors conducted an evaluation of how we manage and control our business. This means our approach to quality assurance, control of records, policies and documents, how we handle an internal audit, control of nonconformity, customer/user complaints and stakeholder feedback were all assessed and validated. We were also assessed against our commitment to quality control, review and implementation of preventative measures.
- Technical Evaluation - A technical evaluation of our systems was conducted to ensure that their programming and performance were in accordance with our policies. The technical evaluation was undertaken by a technical specialist and was subsequent to the policy and quality evaluation.

verifymyage

KYC AVC UK Ltd has been certified by A-LIGN to ISO 27001 under certificate number ISMS-KY-11920 (UK/DE).

KYC AVC UK LTD conforms with the requirements of ISO/IEC 27001:2013 for the scope listed below:

KYC's payment and identity verification services.
Certificate

KYC AVC UK Ltd has received a Seal of Approval from the FSM (DE).

This seal of approval demonstrates clearly that our age verification system is in compliance with German law including specifically the provisions set out in German youth media protection law.
FSM.de