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. und 12.05.2022 in Halle (Saale)

TOP 17: Umsetzung der Anforderungen an ein Altersverifikationssystem (AVS) zur Sicherstellung einer geschlossenen Benutzergruppe nach § 4 Abs. 2 S. 2 JMStV: Bewertung des Konzepts „biometric age detection" der Ondato UAB

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 „biometric age detection" der Ondato UAB 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 „biometric age detection" 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 „biometric age detection" der Ondato UAB 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 „biometric age detection" 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 „biometric age detection"
Mit E-Mail vom 22.03.2022 beantragte die Ondato UAB eine Positivbewertung des Systems „biometric age detection" 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 „biometric age detection"

Bei „biometric age detection" 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 Ondato UAB 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. Im Anschluss an die Alterseinschätzung wird das Bild sofort von den Servern gelöscht. Der Nutzer erhält im Anschluss Zugang zu den jeweiligen Inhalten.

„biometric age detection" 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 Ondato UAB eingereichten Unterlagen verwiesen.

---

4 Bewertung des Systems „biometric age detection"

Bei der Prüfung des Systems „biometric age detection" der Ondato UAB 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 „biometric age detection" 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 „biometric age detection" 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 der mittlere absolute Fehler (MAE) bei liegt. In der Altersstufe von 18-24 liegt der MAE bei 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: Kann das System nicht mit hoher Wahrscheinlichkeit feststellen, ob eine Nutzerin bzw. ein Nutzer volljährig ist, muss die entsprechende Person ein amtliches Dokument vorlegen. Ausweislich des Antrags ist die Zuverlässigkeit der Alterseinschätzung bei den Altersstufen 13-25 größer als Die Ondato UAB nutzt – – die Software des Unternehmens . Es kann somit ergänzend auf die Angaben im Antrag der zurückgegriffen werden. Aus Sicht der Mehrheit der AG „Technischer Jugendmedienschutz" ist für die Ondato UAB davon auszugehen, dass mit einem Puffer von 5 Jahren – wie bei der 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 „biometric age detection" als AVS-Teilmodul einsetzt

Bei dem Konzept „biometric age detection" der Ondato UAB 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 „biometric age detection" 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 „biometric age detection" 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 „biometric age detection" 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 „biometric age detection" der Ondato UAB 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).

Ondato Age Estimation: Introduction

Ondato Age Estimation solution provides a fast and reliable age-checking service that can accurately assess a person's age by analyzing the biometric 3D face map from his/her captured facial image. The solution operates independently from the commonly used process of identity verification and, therefore, does not require identity document validation, biometric data matching, or human expert intervention.

Nonetheless, the Age Estimation tool is designed in a way that allows for additional security steps of user identification in those cases where the system cannot process the captured image or definitively establish the user's age. In such scenario, the Age Estimation solution enables the user to repeat the process once more or go through the complete Photo Identity Verification procedure, which automatically extracts and analyzes the data from the user's identity document, assessing his/her age accordingly.

Ondato Age Estimation: Use Case

The Ondato Age Estimation tool has a wide application in the provision of any age-sensitive goods or services, both online and in person. It also operates as a method to combat social exclusion for a large number of individuals around the world who do not possess a government-issued photo identity document.

For general online use, the Age Estimation tool can be embedded into websites or mobile applications, allowing to receive images of the user's face from a webcam connected to their computer or in their mobile device. This is ideal for controlling access to age-restricted content such as gaming, gambling, and adult material. This is important both in terms of preventing minors from accessing content that might have a negative impact on their mental development, but also in preventing predatory adults from accessing media spaces that are designed for children and teenagers.

User Anonymity and Data Protection

Since the user's 3D face map is the only piece of data that the Ondato Age Estimation tool processes, the actual identity of the user remains completely anonymous. Furthermore, as soon as the age check process is completed, Ondato deletes all collected images, therefore, ensuring user privacy as well as full compliance with the EU General Data Protection Regulation.

It should be noted that none of the gathered facial images are viewed by any Ondato staff members. In GDPR terms, Ondato is only a data processor that provides the Age Estimation service, while the relying parties that use these services are the data controllers. As such, the relying party will decide the lawful basis for their use of facial age estimation under the applicable regulation. Since Ondato has designed the user interface of this solution according to the EU regulatory environment, it ensures that the individual understands the legal terms of the process and provides his/her consent before initiating the Age Estimation.

Age Thresholds Supported by Ondato

The Ondato Age Estimation solution requires implementing a specific target age threshold that online content providers are looking to check their users against.

The currently supported Age Estimation thresholds are:

- ≥ 13 Years ≥ 95% Confidence
- ≥ 16 Years ≥ 95% Confidence
- ≥ 18 Years ≥ 95% Confidence
- ≥ 21 Years ≥ 95% Confidence
- ≥ 25 Years ≥ 95% Confidence

This shows that the Age Estimation tool will return a successful result of the process only if the algorithms have ≥ 95% confidence that the subject user is equal to or exceeds the desired age check threshold.

However, if the user does not immediately pass the Age Estimation process, it does not necessarily mean that the subject is under the target age threshold. It simply means that the algorithms do not have ≥ 95% confidence that the user is over the target age threshold.

Age Estimation Accuracy

Age Group	Gender								
	Female				Male				All
	Skin Tone Types (Fitzpatrick Scale)								
	Type I & II	Type III & IV	Type V & VI	All	Type I & II	Type III & IV	Type V & VI	All	
	MAE	MAE	MAE	Average MAE	MAE	MAE	MAE	Average MAE	Average MAE

The differing MAE shown for the outlined groups (age, gender, skin tone type) correlates strongly with how well-represented those groups are in the training data set. Additionally, it seems reasonable to hypothesize that any error will tend to be higher for older people than younger people, because older people will have been exposed to various unpredictable environmental factors for longer.

Service Configuration for the Client:

The same technical configuration is required for Age Estimation service as is for the Ondato Photo Identity Verification process (KYC API). The Photo Identity Verification solution, therefore, needs to be integrated in order for the Age Estimation check to work. The client needs to contact the Ondato Customer Support for the Age Estimation enablement and provide the required threshold.

Please refer to the API documentation provided here:

Ondato Age Estimation Process: Step-by-Step Guide

End-User Perspective: Visual Representation

1. Legal consent form

Legal version:

Required data
In order to obtain the service from the Service Provider, with this consent I express my agreement that UAB "Ondato" will receive and manage my personal data, including my biometric data, gained from remote identification of my personal identity by taking and/or filming live image of my face, my person's identity or the document used to identify it and/or their image and the personal data contained in them and/or check in the population registry: image of my face, name, surname, nationality, gender, personal code, date of birth, numbers of the document that is being used, date of issue and validity, my signature and the transfer of such data to the Service Provider.

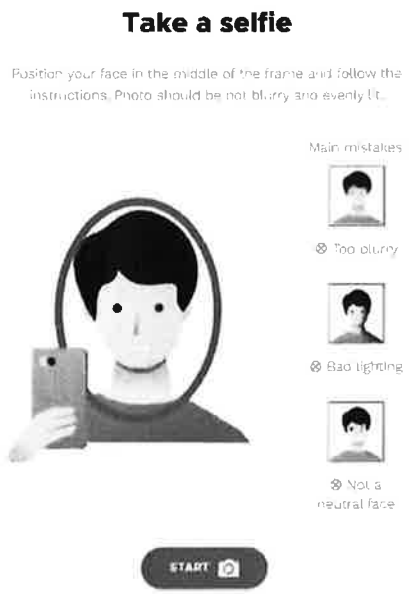
Data processing
I also note that I am informed that the controller of my personal data, including my biometric data, specified in this consent is the Service Provider and UAB "Ondato" will process my personal data only until the remote identification procedure is over and the results will be transferred to the Service Provider. I also declare that I am informed and agree that my personal data obtained for remote identification and its purposes may be stored by UAB "Ondato" for longer period of time than it takes for the identification to be completed or transmission of its results to the Service Provider, but only at the request of the Service Provider or UAB Ondato's contractual obligation to the Service Provider, but not longer than it is defined in the Contract that was signed between UAB "Ondato" and Service Provider or requested by the Service Provider.

Data handling
I am informed, that I can submit request regarding my personal data for more detailed information at support@ondato.com.

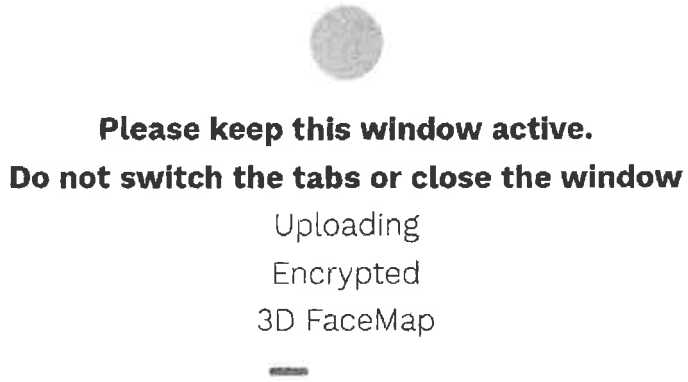
Hereby I declare and confirm, that all the personal data I will provide for remote identification of my personal identity purpose, are correct and accurate, and the document, which I will use for this purpose is not false and valid.

DISAGREE I AGREE

2. Auto-guided liveness check



3. Biometric data processing



4. End-result of the process

Back-Office Perspective: Visual Representation

Biometric age detection

Our system automatically discerns a person's age from a photo or video feed, placing a user in an accurate age group with 95% confidence.

Use cases

Understand your client's age in just a few seconds and request an identity document when in doubt.

Use it as a supplement for your document validation, cross-checking whether the age in ID matches the user's biometric age.

Our biometric age detection solution can be implemented to effectively replace humans that are not as accurate at age estimations.

- AI-powered age verification
- Controls access to age-inappropriate content
- Accurate user's age in seconds
- Fool-proof compliance when combined with ID document

The technology is useful for a wide variety of businesses that are required to verify age before providing a service, from shops selling alcohol and tobacco to cinemas showing age-restricted movies.

How does it work?

The user performs a quick liveness check moving its face around the camera

This generates many photos using various filters to check for spoofing attempts

Using the gathered data, a biometrical 3D map is created

The spatial coordinates from this map are compared, checking in which age group the measurements fit

The user's face is then assigned to one of the age groups with 95% certainty

ondato