

Verifymy Limited – Public Practice Statement

About this Public Practice Statement

This Public Practice Statement provides a certified, informative summary of the Practice Statement identified by Verifymy ISO 27566 Practice Statement Version 1.0 6th February 2026.

The full Practice Statement and the underlying product, process or service has been assessed by the ACCS Certification Scheme and has met the applicable requirements of ACCS 1:2025 and ISO/IEC 27566-1:2025 - Age Assurance Systems - Part 1: Framework in accordance with scope of certification set out on their certificate and schedule.

The full Practice Statement contains sensitive, confidential or security-related information and is therefore not published. This public version provides information about the certified service while protecting information that should not be made publicly available.

For further information about the service, including enquiries about aspects of its operation that are not covered in this public summary, please contact the certified organisation directly.

Name of Client	Verifymy Limited
Public Practice Statement Title	Verifymy ISO 27566 Practice Statement (Public)
Public Practice Statement Version	1.0
Public Practice Statement Date	6th February 2026
Date Certified	21st May 2026



Our mission is to provide frictionless, trustworthy solutions for online platforms to maintain their integrity, protect their reputation and safeguard their users.

Verifymy | ISO 27566 Practice Statement (Public)

Version 1.0

1. Overview

Date: 6th February, 2026

Solution Owner: Verifymy Limited

Product: Age assurance (multi-method)

Verifymy is a global provider of age assurance solutions to relying parties. Our mission is to provide safe, low-friction and privacy-preserving products that can successfully verify 100% of our customers' legitimate end users, whilst preventing all underage users from accessing age-restricted products, content or services.

This practice statement details the operational mechanics of our age assurance methods and algorithms.

2. How it works

2.1. Facial age estimation

This method uses proprietary AI to analyse facial characteristics and determine whether an individual meets a certain age threshold.

To complete the age check, the end user must take a short selfie video, which is then submitted securely using 256-bit encryption to the Verifymy server. Instructions and user prompts are provided within the user flow.

During the user's short selfie video, two separate processes occur. Firstly, our proprietary liveness anti-spoofing checks will work in the background to ensure a live person is operating the camera.



VERIFYMY LIMITED, Unit 213, The Frames, 1 Phipp Street, London, England, EC2A 4PS. Company number: 12050874. VAT number: 330383724.
We are ISO 27001 Certified. VERIFYMY LIMITED has been certified by A-LIGN to ISO 27001 under certificate number ISMS-KY-11920.

Secondly, our proprietary AI age estimation model determines whether an individual meets a certain threshold e.g. ± 18 . The model has been trained using a variety of different data inputs, all of which have the relevant consent requirements in place.

The solution can return a **'YES'** response, where the user is estimated to be over the age of interest e.g. 18+, or a **'No'** response, where the user is not permitted to gain access to the website or app.

2.2. Email-based age check

This method uses AI to analyse the usage of a user's email address across websites and apps, to determine whether an individual meets a certain age threshold.

To complete the age check, the end user's email address can be submitted in one of two ways:

- Via a relying platform's API. In this instance the user must be logged in to an account, where ownership of their email address was authenticated at the point of account creation
- Manually inputted by the end user

The email address is submitted securely using 256-bit encryption to the Verifymy server. Instructions and user prompts are provided within the user flow.

Verifymy analyses the email address using both proprietary algorithms and third-party databases. Our AI model analyses the outputs to establish whether an individual meets a threshold e.g. ± 18 .

Where the user has manually entered their email address, they must complete a SSO/OTP process before a successful check can be completed.

The solution can return a **'YES'** response, where the user is estimated to be over the age of interest e.g. 18+, or a **'No'** response, where the user is not permitted to gain access to the website or app.

2.3. Identity document scan with face match

This method first requires the user to take a selfie in order to capture an image of their face. The user must then provide an image of a government-issued identity document, using a smartphone or other webcam.

The images are submitted securely using 256-bit encryption to the Verifymy server. Instructions and user prompts are provided within the user flow.

This government-issued document is processed with proprietary and third party technology to



extract data from the Machine-Readable-Zone to determine whether the user is over the age of interest e.g. +/-18.

If a positive result is received, Verifymy's proprietary technology then compares the user's image in the identity document with the captured selfie.

The solution can return a **'YES'** response, where the user is verified to be over the age of interest e.g. 18+, or a **'No'** response, where the user is not permitted to gain access to the website or app.

2.4. Credit card check (currently commerce only)

This method requires the end user and/or platform to provide a credit card number, expiry date, CVC, cardholder name and billing address to the Verifymy flow, which are submitted securely using 256-bit encryption to the Verifymy server. Instructions and user prompts are provided within the user flow.

A temporary charge is placed on the card that is later refunded. The credit card information is referenced with a third-party supplier in order to validate its authenticity.

The presence of the credit card information on the third-party database confirms that the end-user has previously verified their age and identity with the credit card provider.

The cardholder's name is cross-checked against the transaction details provided by the commerce site. If the transaction succeeds and the name matches, a **"yes"** response is returned and the user is successfully approved as being 18+.

2.5. Mobile phone check

This method requires the end user's mobile phone number in order to determine whether an individual meets a certain age threshold.

To complete the age check, the end user's mobile number can be submitted in one of two ways:

- Via a relying platform's API. In this instance the user must be logged in to an account, where their mobile phone number was authenticated at the point of account creation
- Manually inputted by the end user

The mobile number is submitted securely using 256-bit encryption to the Verifymy server. Instructions and user prompts are provided within the user flow.



Verifymy uses third-party suppliers to establish various information. Firstly, we can confirm the adult content bar status of the submitted mobile telephone number. We can also query MNOs or other third-parties in order to determine whether the owner of that number is 18+ based on a previous identity verification check.

When the user has manually entered their mobile number, an OTP must be retrieved before a successful check can be completed. This is to prove ownership of that mobile phone number

The solution can return a **'YES'** response, where the user is determined to be 18+, or a **'No'** response, where the user is not permitted to gain access to the website or app.

2.6. Credit reference check (currently commerce only)

This method matches an end user's name and address with a third-party credit reference bureau.

Verifymy receives the end user's name and address via a marketplace or ecommerce site's transactional API, submitted securely using 256-bit encryption to the Verifymy server. Instructions and user prompts are provided within the user flow.

The end user's details are taken from an age-restricted transaction, meaning the address matches the location that the item will be shipped to, ensuring that another person's name and address cannot be fraudulently used to circumvent the age check.

The presence of the end-user's name and address on the credit reference bureau's database confirms the end-user is 18+ and a **"yes"** response is returned.

2.7. Double-blind check

This method requires the end user to download a third-party application widely available in the major App Stores.

Within the application the user must then create an account by uploading a government-issued identity document and capturing a selfie to match their face with the image within the identity document.

When an end user selects the double-blind method within the Verifymy flow a dynamic age verification session is launched by displaying a QR Code or Magic Link on the screen.



The user can then open their third-party app and select the option to scan the QR Code on their screen and their anonymous age credential is then shared with the relying platform..

In line with the principles of double blind age checks, throughout the process neither Verifymy nor the relying platform knows or sees any identifying information of the end user.

2.8. Verifymy account log in (reauthentication)

This method is available to end users who have successfully proven their age using Verifymy and have subsequently chosen to set-up a Verifymy account, anchored to an email address or mobile phone number.

If a user has previously created a Verifymy account, they may be presented with the option to sign-in to that account and reauthenticate rather than completing a new age check.

Having selected this method and after signing in with an alphanumeric or biometric password, Verifymy prompts the user to complete 2FA. This ensures that the user has access to the email account or mobile phone number and mitigates the possibility of users sharing or selling log-in details.

Successful 2FA reauthenticates the user as that same user who initially successfully underwent the initial age check, AV process with provider and a positive **“yes”** response e.g. 18+ confirmation is returned to the relying platform.

3. Privacy and Data Protection principles:

- Our solution has been audited and certified by the [Age Check Certification Scheme](#) as being compliant with GDPR and UK GDPR. All data is stored within the EU and we meet all relevant storage and transfer requirements. No data is stored on minors. Our full privacy policy and biometric privacy policy is available on our website.
- Privacy by design: the solution was built from the ground up with privacy in mind.
- Data minimisation: We collect and process only the minimum amount of data needed to fulfil the requirements of our safety tech solutions. We routinely evaluate our data collection policy to ensure we adhere to data minimisation principles.
- Data retention: all captured data is encrypted, and Personal Identifiable Information (PII) is typically deleted after a maximum 28 days, although this is often as soon as the check is completed dependent on local regulatory requirements and/or commercial agreements.



- Data integrity: 256-bit encryption is the highest level of encryption possible, maximising the security of all captured data. Anonymisation via hashing and salting data adds an extra layer of security and confirms the integrity of data.

4. Continuous Improvement:

The systems are kept under continuous and regular review in the following ways:

- Top Management Oversight: leadership actively monitors system effectiveness and ensures alignment with strategic goals.
- Management Reviews: scheduled assessments evaluate system performance, customer feedback, and regulatory compliance, with updates implemented as needed.
- Internal Audits: regular audits check compliance with quality and legal standards, using KPIs like service availability, data retention, and accuracy.
- Corrective & Preventive Actions: issues are identified and resolved through a structured Corrective and Preventive Action system to prevent recurrence and improve processes.
- Document Control & Change Management: policies and procedures are regularly reviewed, updated, and controlled to maintain relevance and compliance.
- Internal Communication: employees engage in quality improvement through meetings, data analysis, and an open-door policy for suggestions.

These mechanisms ensure continuous improvement, regulatory compliance, and effective system management.

5. Fallbacks & overrides

Verifymy always recommends that relying platforms deploy multiple age check methods, thus ensuring users can continue to prove their age should one individual method be unsuccessful or suffer any period of downtime.

We also have a back-up platform service should our primary cloud computing hosting service suffer any performance issues.

In line with GDPR Article 22, end users using our solution to determine their age have the right to request human intervention and a manual review of any automated decisions. We provide contact details of how users can make this request within our Age Assurance Privacy Policy.



6. Indicators of effectiveness

6.1. Facial age estimation

- IEEE 2089.1 2024 – (ACCS)

6.2. Email based age checks

- ISO/IEC/IEEE 29119-3:2013 – (ACCS)

6.3. Identity document scan with face match

- Third-party accuracy performance metrics disclosed

6.4. Credit card check

- Third-party accuracy performance metrics disclosed

6.5. Mobile phone number check

- Third-party accuracy performance metrics disclosed

6.6. Credit reference check

- Description of third-party processes and mechanics disclosed

6.7. Double-blind check

- Third party does not currently publish any performance data

6.8. Verifymy account log-in (reauthentication)

- The accuracy of the age check result is directly related to the accuracy of the initial check before the account was created. Account log in and 2FA protects against circumvention.

7. Publicly available specifications

Verifymy has, or recently has had, the following certifications or endorsements:

- ISO 27001 – international standard for information security management systems (ISMS)



VERIFYMY LIMITED, Unit 213, The Frames, 1 Phipp Street, London, England, EC2A 4PS. Company number: 12050874. VAT number: 330383724.
We are ISO 27001 Certified. VERIFYMY LIMITED has been certified by A-LIGN to ISO 27001 under certificate number ISMS-KY-11920.

- PAS 1296 - Code of Practice for online age checking services (ACCS)
- IEEE 2089.1 2024 - Facial Age Estimation (ACCS)
- ISO/IEC/IEEE 29119-3:2013 - Email-based age estimation (ACCS)
- General Data Protection Regulation (ACCS)
- Arcom SREN compliance (ACCS)
- KJM approval (ID scan + face match, facial age estimation, credit reference bureau, credit card, Verifymy account reauthentication)

8. Contact Details:

Andy Lulham

andylulham@verifymy.io

Certified Summary

