

Primary Contact Details

Company Name

Yoti

Solution Name

Yoti Age Verification

Company Logo

- [yoti-logo.png](#)

Lead Contact

Lead Contact Email

Lead Contact Phone (with country code)

Please describe how your system and practice statement are kept under continuous and regular review, including by your top management

Yoti Age Verification allows a relying party to request an age assurance check from an individual

- Without requiring persistent storage of any personal information
- Without requiring the individual to share personal information with the relying party
- Without requiring the individual to grant use of their personal information for any reason other than age verification
- Without requiring the individual to generate a traceable footprint.

The age portal provides a relying party the means to generate a one time age assurance request that is tailored for each individual circumstance, such that different verification options can be provided based on the services offered to the individual, the device type, predicted location and any other external conditions that may impact the verification process. The portal does not mandate any use of methods, this is decided in the first place by the relying party and finally by the user.

As an organisation we have multiple layers of processes, to ensure the system operates as described.

All changes to production systems are tested thoroughly during the development process by our QA team across multiple test environments to ensure that quality is maintained and new features meet the defined requirements.

There is a separation of concerns, meaning the people making changes to system behaviour can not input changes into the production system. This separation is enforced by technical controls and requires sign off

from various stakeholders before a release to production is performed.

Staff receive regular training to ensure they understand how to comply with security and privacy requirements.

The information in this practice statement is reflected in the policies that are used to meet national and internationally recognised standards. There are yearly audits to ensure Yoti follows its documented processes to satisfy claims relating to

- Age Checking
- Security
- Privacy
- Data handling
- Business operations

The outcome of each audit is presented to Yoti's senior management team.

Are you

Age Assurance Provider (an entity responsible for providing age assurance results to a relying party)

Practice Statement by Age Assurance Provider

Age eligibility requirements

The age assurance check may return results evaluating if a user is:

- An individual is over an age threshold e.g. 13+, 16+, 18+
- An individual is under an age threshold e.g. Under 18
- The age in years, of an individual e.g. 16 years
- The age range, of an individual e.g. 13-17 years

The relying party configures a threshold for each method individually when they request an over/under result. Additionally, they set the configuration of the age check for each age assurance session so they have flexibility to select the methods available and their thresholds for a user, in a given jurisdiction.

Age assurance components

Facial age estimation

The source of the age verification data is the image taken by the individual at the time of the check. The age of the user is estimated using Yoti's facial age estimation technology which uses just the image of the face in order to estimate the age. To support this, there is also a liveness check to make sure that it is a genuine image captured at the time of the check (not a photo, video or mask). This has been independently tested by NIST (National Institute for Standards & Technology) and the ACCS (Age Check Certification Scheme) for accuracy; this approach has the seal of approval of the FSM in Germany (the The German Association for Voluntary Self-Regulation of Digital Media Service Providers) and is listed on the KJM (Commission for Youth Media Protection) Raster in Germany. The image used for facial age estimation is not saved, shared or used for any other purposes. Facial age estimation is not facial recognition because it can't uniquely identify the user; it simply estimates their age from an anonymised image.

The Yoti facial age estimation white paper <https://www.yoti.com/blog/yoti-age-estimation-white-paper/>, provides details on the accuracy of this approach.

Digital ID

If an individual has registered for a Digital ID, they can use this to share either a year of age, a confirmation

of age over or a confirmation of age under (e.g. 18+, or under 18). This can be done without providing any additional information to a relying party.

The user's proof of age will be backed by one of several potential sources - the identity document that they add during registration or alternatively, if accepted by the relying party, can be from a facial age estimation performed in the app or from an mDL (mobile driving license) credential.

In order to share this information a user will be asked to scan a QR code or press a button linking to their Digital ID to start the age verification process. When the Digital ID opens, the user is informed what data has been requested and who will see the data. The user is given an option to approve and reject the request for proof of age. The user's proof of age is only shared with the relying party if the user approves the request.

Age extracted from a government issued identity document

A person can use an approved ID document that has a photo and strong security features to verify their age.

The user is asked to provide the type of document, country of issue, an image of their document and a selfie. If the selfie matches the photo on the document and both images appear to be genuine, the date of birth on the document is processed to establish the document holder's current age. The captured images and extracted data are immediately destroyed. Just the derived age result is returned to the relying party, e.g. 18+.

Age tokens

Reusable age tokens are added to the user's browser when their age has been verified by Yoti. Age tokens give users continued access to your site without having to prove their age again, meaning less user friction and lower costs.

Tokens don't contain any personal details, just the result of an age check and information around when and how it was performed. A website can define what type of age tokens they will accept based on the requirements in each jurisdiction.

Indicators of confidence

Yoti takes several steps to ensure confidence in results. All relevant steps must pass for a positive result to be returned.

Thresholds

Yoti's facial age estimation white paper provides relying parties an understanding of the risk of a facial age estimation returning an incorrect result. Using this information, a relying party can adjust their usage of Yoti's facial age estimation to minimise the risk of a false positive.

Single person

We take steps to ensure we only process data from a single person. If multiple people are detected, the process stops. This ensures the age result is provided for the correct person.

Image quality

The quality of the captured image is assessed to ensure that there is sufficient clear information to make an age determination.

Liveness

A liveness check, this ensures that the face captured is that of a real live person and not a fake image e.g. photo, image from a device screen, video of a person's face or a mask.

Anchoring

When accepting an age from a document, the relying party is encouraged to configure the check to require a face match with liveness check to ensure that an individual is not using someone else's document.

Document authenticity

When accepting an age from a document, checks are performed to confirm the presence of the security features expected.

Binding process

The process of binding an individual to an age check depends on the method(s) made available by the relying party and the method chosen by the individual.

Facial age estimation

There is little information to collate. Yoti takes three crucial steps as part of the facial age estimation process:

Ensure only one face is presented.

Ensure the face is a live face. This process involves checking to ensure that the estimation process is not being used on a printout, a picture from a screen, a video or someone wearing a mask.

Ensure the face was captured by the expected input device. This process is designed to detect attempts to inject false or manipulated data into the device's hardware.

Digital ID

To use Yoti's Digital ID app, or an affiliated Digital ID Connect app, the user must register their identity using the personal device. The information they register is verified one time by matching their face to the face on their document using facial recognition. If it is possible to read an NFC in the document we can further ensure that the document is real and in the possession of the individual. After the initial verification, the data attributes e.g. date of birth, name, age, are each encrypted and stored separately with the location and decryption details placed in a secure store on the user's personal device. The app itself must then be secured with a PIN or a biometric. When the user wants to verify their age using their Digital ID, the user must:

Log into their device

Log into their Yoti Digital ID

Consent to share their age and only their age

This will allow their device to then provide the location of and decryption details of their age attribute.

The process provides strong evidence that the individual is using a device they control, with an account they control, with their consent, with data that has been verified to be accurate.

Age from a document

To use the age portal to verify an age from a document, the relying party is encouraged to request a face match with liveness check to ensure that an individual is not using someone else's document.

In this scenario the binding process is:

1. Request a document to be presented
2. Check the document appears to be a valid (e.g. follows the correct template for the specific document presented e.g. a passport or a driving license or a national ID card)
3. Check to see if the document appears to be a real document and not a print out or screenshot etc

4. Capture the face of the person presenting the document
5. Ensure the face is a live face. This process involves checking to ensure that the estimation process is not being used on a printout, a picture from a screen, a video or someone wearing a mask
6. Ensure the face was captured by the expected input device. This process is designed to detect attempts to inject false or manipulated data into the device's hardware.
7. Make sure the face captured (in step 4) matches the face found on the document (presented in step 1).

Privacy and data protection

The solutions provided are designed to not require the storage of any personal information after a verification is complete. This approach to system design is regularly reviewed internally and externally to verify that personal information gathered for age assurance purposes is not stored after an age verification is completed or shared with the relying party.

Staff requiring either access to sensitive data or access to systems that can read or modify sensitive data must have their access requirements clearly documented as part of their job role. Job roles are regularly reviewed to ensure appropriate access restrictions are in-place.

Regular training is provided to Yoti members of staff to ensure they understand their responsibilities in keeping data secure and protecting privacy.

The following policies ISO 270001, ISO 277001, PAS 1296:2018 and SOC2 Type 2 contain our privacy and data handling policies; they are available to auditors. We are audited externally against these standards and have an internal process of reviewing our continued adherence to these policies.

Ease of use

The age assurance solutions provided are designed to be as simple and accessible as possible, meeting the WCAG 2.2 AA Accessibility standards. In addition, the solution has been designed in line with the principles of the UK ICO's Age-Appropriate Design Code, ensuring not only enhanced privacy protections but also the use of clear and simple language for better accessibility and understanding.

Security

ISO 270001 and SOC2 Type 2 contain our security policies. We run a security bounty program to engage with ethical hackers in discovering security challenges.

Staff requiring either access to sensitive data or access to systems that can read or modify sensitive data must have their access requirements clearly documented as part of their job role. Job roles are regularly reviewed to ensure appropriate access restrictions are in-place.

Automated systems are used to monitor Yoti's internal operations for signs of suspicious behaviour.

Regular training is provided to Yoti members of staff to ensure they understand their responsibilities in keeping data secure and protecting privacy.

Security efforts are supported by

- An in-house security team
- A security forum consisting of representatives from across the organization
- Regular external penetration tests
- External threat analysis
- Automated security scans
- Mandatory staff training
- A supplier due diligence and regular supplier audit process ensuring that third and fourth party suppliers do not misuse data or pose security risks.

Human rights protections

The role of the Yoti internal ethics committee is to review proposed changes to products or business practices and consider the positive or negative intended or unintended consequences and ethical implications. This committee consists of representatives from across the company.

We also engage with the external Yoti Guardian Council. This is a rotating committee of external subject matter experts who meet on a quarterly basis to discuss Yoti's business and technology operations and plans. They have the opportunity to discuss with staff members about projects that have been released, are in development or are planned. We invite their scrutiny and give them the opportunity to raise questions and give advice. The minutes of these meetings are published openly.

Yoti has a clearly defined whistle blower policy and a way for all staff to anonymously report any concerns they have about how the company is operating.

Through the use of the internal ethics committee, the external Guardian Council and our staff training and policies, including the whistle blower policy, the rights of individuals are considered and supported across all stages of the product development and the company's operational cycle.

Audit, certification and review

Yoti is externally audited by independent third parties to ensure we are following our security and operational risk policies as defined: ISO 270001 ISO 277001 ISO 9001 SOC2 Type 2 PAS 1296:2018

External audits are performed yearly by one of the big 4 accounting firms.

There are internal audit and quality management processes running constantly, which include department selection and staff interviews.

We submit updates to certification and testing organisations, to review how effective our solutions are.

Age Check Certification Scheme:

- Age assurance

National Institute of Standards and Technology:

- Facial age analysis global benchmarking
- Face matching, used to bind a face to a document
- Presentation attack detection

Since 2019 we have been publishing white papers detailing the accuracy of our age estimation models

<https://www.yoti.com/blog/yoti-age-estimation-white-paper/>