

UAB Ondato – Public Practice Statement

About this Public Practice Statement

This Public Practice Statement provides a certified, informative summary of the Practice Statement identified by Practice Statement for Age Verification Services (ISO27566) v1.3

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	UAB Ondato
Public Practice Statement Title	Practice Statement for Age Verification Services
Public Practice Statement Version	1.3
Public Practice Statement Date	Effective: 2026-10-21
Date Certified	10 th September 2026

UAB “ONDATO”

Practice Statement for Age verification services

Ver. 1.3

Date: 2026-10-21

Effective: 2026-10-23

Document metadata

Prepared	CISO – Dmitrij Olifer
Reviewed	DPO – Rūta Bučinskaitė, CTO – Gediminas Letulis
Approved	COO – Olga Šimkuvienė

Version control

Version no.	Date	Author	Description of the changes
1.0	2025-11-10	D. Olifer	Initial version
1.1	2026-07-07	D. Olifer	Amended according to auditors comments
1.1	2026-08-03	D. Olifer	Added context in which an age assurance system can be used.
1.2	2026-09-25	D. Olifer	Practice Statement amended to be aligned with SAFE for Kids Act
1.3	2026-10-21	D. Olifer	Amended used technical components (WebSDK, Mobile SDK and onAge versions)

Location

Version no.	Classification	Published
1.3	Public	https://www.ondato.com/age-verification-practice-statement

Content

Document metadata	2
Introduction.....	4
Scope.....	4
Governance.....	6
Age eligibility requirements.....	8
Age assurance system indicators of effectiveness.....	9
Age assurance components	10
Indicators of confidence.....	14
Binding process	15
Privacy and data protection.....	16
Ease of use	18
Security measures	20
Human rights protections	21
Audit, certification, and review	22
Contact details.....	22

Introduction

This document is the Practice Statement for Age verification services (hereinafter Statement) of the UAB “Ondato” (from now on, Company). Company is concentrating on Identity validation and proofing, Age estimation and verifications services for Trusted Service Providers, Financial Institutions and Private Companies. Statement sets out Company’s end-to-end approach to Age Assurance so that clients, including and children, could safely access appropriate solution and services while their rights and privacy are protected.

Statements defined in this document transfer defined goals into operational, auditable procedures, making clear what Company do, when do it, and what evidence Company capture, store and process.

The document provides a single source of truth for product, legal, IT, security, and audit teams, and a common basis for engagement with regulators and partners.

Scope

Scope of the statement is limited by Age assurance solution and services, including Age estimation and Age verification, provided by UAB “Ondato”, which is implementing Age Assurance Provider functions for their Customers.

New York context of use: this statement includes age assurance supporting covered online platforms under the New York Stop Addictive Feeds Exploitation (SAFE) for Kids Act and 13 NYCRR Part 700.

Covered Jurisdictions:

The Company provides online age assurance services within the European Economic Area,

- the United States,
- Canada,
- Australia,
- Brazil,
- Mexico,
- Peru,
- Argentina,
- Jamaica,
- and Qatar.

Industries sectors in the scope:

The services are intended for:

- adult-content websites,
- gambling and betting services,
- online gaming,
- social platforms,

- and other online services that must determine whether an individual meets an applicable minimum-age threshold.

The service primarily uses biometric age estimation based on the analysis of a facial image. Where age estimation fails, produces an inconclusive result, or does not satisfy the threshold configured by the Customer, document-based age verification may be used as a fallback method. The service scope includes facial-image capture and processing, generation of age-estimation results, document validation used as a fallback, related application programming interfaces, software development kits and user interfaces, and the infrastructure, monitoring, logging, security and operational processes required to support service provision.

Other Company services that are not directly related to the age assurance services described in the applicable Practice Statement are outside the service scope. This includes, among others, Know Your Business, general customer onboarding and monitoring, authentication, document signing, content moderation and compliance-screening services. Customer-owned websites, applications, content-management systems, access-control mechanisms and decisions made by the Customer on the basis of the age assurance result also remain outside the scope. Customer-owned platforms and their access, feed and notification controls remain outside Ondato's certification boundary, but the New York profile defines mandatory integration dependencies. Optional reusable authentication is excluded from the New York profile unless separately assessed and included in the approved certification and data-protection scope.

Assumptions, Preconditions, and Operational Conditions

No specific environmental or demographic conditions are established as mandatory preconditions for the use of the service. However, successful operation requires an internet connection, a supported device, an operational camera and image quality sufficient for facial-image or document processing. The service is intended only for online use. No specific age group is technically excluded, although the Customer remains responsible for determining whether the use of the service is lawful and appropriate for its users and for applying any required safeguards. The supported age assurance methods are limited to biometric age estimation and document-based age verification as a fallback. Any other age assurance methods are outside the scope.

The biometric age-estimation process does not normally rely on external authoritative or secondary data sources. During the document-based fallback process, a government-issued identity document is used as the primary source for confirming age. In certain supported jurisdictions, document details may also be checked against supplementary sources. For example, in Lithuania, a document may be checked against the Lost and Stolen Documents Register.

Before service provision begins, the Company and the Customer enter into the applicable contractual arrangements, including the General Terms and Conditions, relevant

service documentation, a Data Processing Agreement and an annex describing organisational and technical security measures.

The service relies on several third-party technology and infrastructure providers, including Microsoft Azure for cloud infrastructure, FaceTec for facial-processing and liveness-detection technology deployed within the Company's infrastructure, Cloudflare for network and application security, IPstack and IPinfo for IP geolocation and enrichment, and Shield for device-intelligence and device-fingerprinting capabilities. These third-party services support the operation, security, fraud prevention and resilience of the age assurance service but do not independently determine an individual's age.

New York context and certification boundary

The profile supports determination of whether a covered user is under 18 or at least 18 for controls on addictive feeds and notifications concerning those feeds between midnight and 6 am Eastern. Clients must assess whether their service is an addictive online platform.

The client determines territorial coverage using all reliable available location information and investigates location concealment. IP geolocation alone is not assumed sufficient. The client owns feed and notification enforcement, actual-knowledge assessment, user appeals and any parental-consent system. Ondato provides the contracted method, secure result binding, supporting records and technical assistance. Contractual allocation does not remove statutory duties: covered operator includes relevant agents and affiliates, and outsourcing does not reduce obligations.

The New York assessment boundary includes Ondato's facial age estimation and document-based age verification, capture, liveness and circumvention controls, age calculation, session binding, APIs, SDK and web interfaces, relevant infrastructure and supplier components, monitoring, support, data lifecycle and governance. Each deployed method, model, release, setting and fallback arrangement are identified in the certification scope.

Customer feed and notification systems, territorial applicability decisions, actual-knowledge assessment, appeals and any parental relationship and consent service are external integration dependencies. The age-status component for a parent may be included where contracted and assessed; a complete parental-consent service is not established by the supplied baseline. Outsourced components remain assessable where they support the age assurance method.

Optional reusable authentication, PIN/device-fingerprint reuse and persistent biometric enrollment are excluded from the New York profile unless specifically assessed for necessity, privacy compliance and certification coverage. No zero-knowledge age-proof capability is asserted.

Governance

Company maintains this practice statement and the Age assurance solution by applying structured operational and security management approach that includes:

- Governance;

- Risk management;
- Stakeholder feedback;
- and continual improvement.

Management reviews for Age Assurance solution are performed at least annually, after major incidents, or major modification in solution or service design, infrastructure or functionality. During Management reviews responsible persons, such as Product Owner, Chief Technology Officer, Chief Information Security Officer, Data Protection Officer, presenting to the Management overall state and status related to the solution and services, including but not limited by:

- Regular Evaluation and Monitoring
 - Internal assessments of the practice statement. The assessment is an evaluation of whether the practice statement continues to align with the business objectives, customer commitments and regulatory requirements.
 - evaluation of performance (including fairness, accuracy and unintended bias);
 - Information about incidents or outages;
- Feedback from internal and external interested parties and stakeholders
 - Legal;
 - External and Internal auditors;
 - Regulators;
 - Potential customers.

As a result of Management review Company defines: corrective actions, operating-point updates, and this statement's redlines.

Company maintains a formal governance structure for the Age Assurance solution and services. And this structure incorporate such roles:

Role	Function
Product Owner	Overall accountability for solution and service
Chief Technology Officer	Technical solution and service development and maintenance
Chief Information Security Officer	Security best practices implementation and control.
Data Protection Officer	Data protection and Privacy, including Data Protection Impact Assessment, implementation and control.

This Practice Statement is version-controlled with an effective date, change log, and approval record.

Age eligibility requirements

As an Age Assurance Provider offering facial age estimation and verification services, we support relying parties in meeting their age eligibility requirements by providing probabilistic age estimation and verification results, typically expressed as an age estimate and age range or a binary response, with some level of deviation (up to 3 years), stating that the user is above an age threshold or not, along with a confidence level.

For the New York profile, the legal age boundary is 18; any estimation buffer or operating point must be specifically validated and certified. A general deviation or mean age error is not a substitute for the statutory false-positive and total-accuracy thresholds.

These outputs enable the relying party to make determinations aligned with applicable policies or legal mandates, without us directly enforcing eligibility decisions.

The solution and services provides to the Company's clients such functionality as:

- determination whether a user meets or fails a defined age threshold;
- receive probabilistic age estimation outputs with confidence;
- receive exact-age or jurisdiction-sensitive attributes where required by applicable regulations and Client's policy;
- simplification of further age verifications for the Clients.

New York age status decisions

Actual knowledge of minor status includes an attributable minor self-declaration, a qualifying method's minor result, held/accessed commercial data which would yield a minor result if applied to an offered method, and other reliable evidence. A later adult result does not simply erase that knowledge. The company investigates conflicting results and use the appeal route where appropriate.

An adult determination requires the qualifying offered methods and an adult result from at least one, without contrary actual knowledge. The exceptional adult presumption applies only when all offered qualifying methods have been completed, including at least one meeting the total accuracy minimum, every method is genuinely inconclusive, and no actual knowledge of minor status exists. Refusal, incomplete input, technical error and circumvention do not satisfy that route. Record presumption as an operator decision distinct from a method-confirmed adult result.

When government identification is offered, the operator accepts identification from all US and non-US jurisdictions. The supported-document list and an appropriate handling route are verified before deployment. Offer a non-government-ID method unless the specific other-law or zero-knowledge exception applies. Permit appeal where all other offered methods are inconclusive and the user declines government ID.

Age assurance system indicators of effectiveness.

The Company's standard-build age assurance solution satisfies the "Highly Effective" compliance criterion defined in the IEEE 2089.1 standard. To achieve this, the age assurance system must satisfy the following criteria:

- Provide at least 95% accuracy based on:
 - testing with more than 300 subjects
 - testing across 3 different skin tones
 - testing both genders.

For the New York profile, effectiveness is assessed against the age-specific accuracy and circumvention criteria in §§700.1(b), 700.1(gg), 700.4 and 700.5.

- The New York assessment measures false positives separately for ages 0–7, 8–13, 14–15, 16 and 17, with the limits set out in the New York requirements in this statement.
 - Test sample sizes was justified for high confidence and low error using the latest US Census Bureau population of New York as the baseline.
 - Image datasets represents varying photographic conditions, presentation, pose and facial archetypes, and not overlap substantially with training or tuning data.
 - Testing covers adult false negatives, inconclusive outcomes, circumvention, data controls, encryption and security.

New York certification and performance requirements

Each offered age assurance method receive annual certification from an accredited third party recognized by ANSI or an equivalent accreditation body. The certification covers ISO/IEC 27566-1:2025, IEEE 2089.1 (2024), or an equivalent industry standard, the accuracy minimum and the testing required by §700.5(b). Every offered method meet the accuracy minimum and at least one must meet the total accuracy minimum.

Minor age	Maximum false positives	Maximum false positives plus inconclusive
0 to 7	0.1%	0.1%
8 to 13	1%	1%
14 to 15	2%	2%
16	8%	8%
17	15%	15%

For the accuracy minimum, false-positive rates exclude failures/refusals to supply data and inconclusive outcomes. For the total accuracy minimum, false-positive and inconclusive outcomes are combined; failures/refusals are excluded. Each minimum also requires at least 98% method-circumvention detection. A false positive means a minor classified as adult.

The report must include protocols and all results: false positives for ages 0–17 in aggregate and the required bands; inconclusive rate and reasons; adult false negatives in aggregate and ages 18, 19–20, 21–25 and 26–30 and circumvention testing against a recognised standard, such as IEEE 2089. Test results, reports and certificates are preserved for at least 10 years.

Age assurance components

Company's standard-build age assurance solution does not rely on credentials or authoritative identity sources, but instead uses biometric-based, non-intrusive inference to estimate the age of an individual, through utilizing:

- in-house developed age estimation algorithm;
- age estimation and verification algorithm and solutions provided by trusted suppliers.

However, for the Clients who require High confidence or require reusability of the age verification results, Company's solution and services has extensions, which in case of need allows to:

- validate persons document (for high-confidence);
- check the information provided in the in the document against trusted sources, such as government registries (for high-confidence);
- create account, PIN and device finger print to ensure further access to the system for the person, who successfully passed age verification (easy-use)

Company's in-house developed algorithm, was independently tested and validated by NIST, according to their Face Analysis Technology Evaluation (FATE) Age Estimation & Verification framework. More details could be found here: https://pages.nist.gov/frvt/html/frvt_age_estimation.html

Age Assurance solutions is utilizing such component:

- **Age estimation method:**
 - **Algorithm-based facial age estimation:** medium assurance suitable for threshold checks with calibrated operating points. We deploy in-house developed and trusted supplier provided algorithms and models for facial analysis. This models trained on diverse datasets to estimate a user's age or age range from a facial image or video. The output is typically a predicted age with confidence-weighted range, or a binary output (stating that the individual is above a certain age given as a

threshold). The method does not require access to government-issued IDs or any other authoritative sources.

- **Document/identity-backed verification:** higher assurance when an authoritative source is required. In addition to validate age could be used person identity document. By default, the flow validates the document issue date and informs the user if the document has expired. Age estimation with expired documents is not allowed, and the process is terminated with a failure status.

In addition data captured from the document is validated against data coded in MRZ code.

Company is utilizing PRADA DB to define documents templates and security measures need to be validated during the document check.

As an additional check, the data presented in the document is captured and validated against trusted data sources, such as government registries, where such registries are available for validation of document revocation or suspension.

- **Data source:**

- our system uses facial imagery (primary biometric signal) provided in real-time by the user, typically captured through a camera at the point of interaction. No persistent identifiers are retained, unless explicitly configured by the relying party and in accordance with applicable data protection regulations.
- data provided in the person identity document (passport ID card).

- **Age inference method:**

we do not deploy secondary inference method (e.g.: device usage pattern) as part of the age assurance result. Our focus is exclusively on direct facial estimation of person or validation of his document.

Fallback and escalation paths are available when captures are inconclusive or fail liveness checks. Company can be deployed with one or a combination of the above, subject to legal basis, data protection rules, and customer configuration.

Company provides to the Clients Web SDK or Web application options:

- Web SDK is could be integrated by the Clients to their own communication with customers solutions, such as Web or Mobile application. Web SDK is provide to the Clients flexibility to integrate Company's solution to the Client's ecosystem and make it looks as native for their Customers;
- Web application is implemented in form of iFrame, which could be integrated to the Client's website.

Age Assurance solutions results could be visible in the Dashboard configured for each client, or in case of need Age Assurance results could be captured from Company's solution by utilizing standard API's approach.

Currently company provides such technical components as part of its solution:

- Web SDK - v2.3.0;
- Mobile SDKs - v3.63;
- Age estimation solution (OnAge) - v1.0.

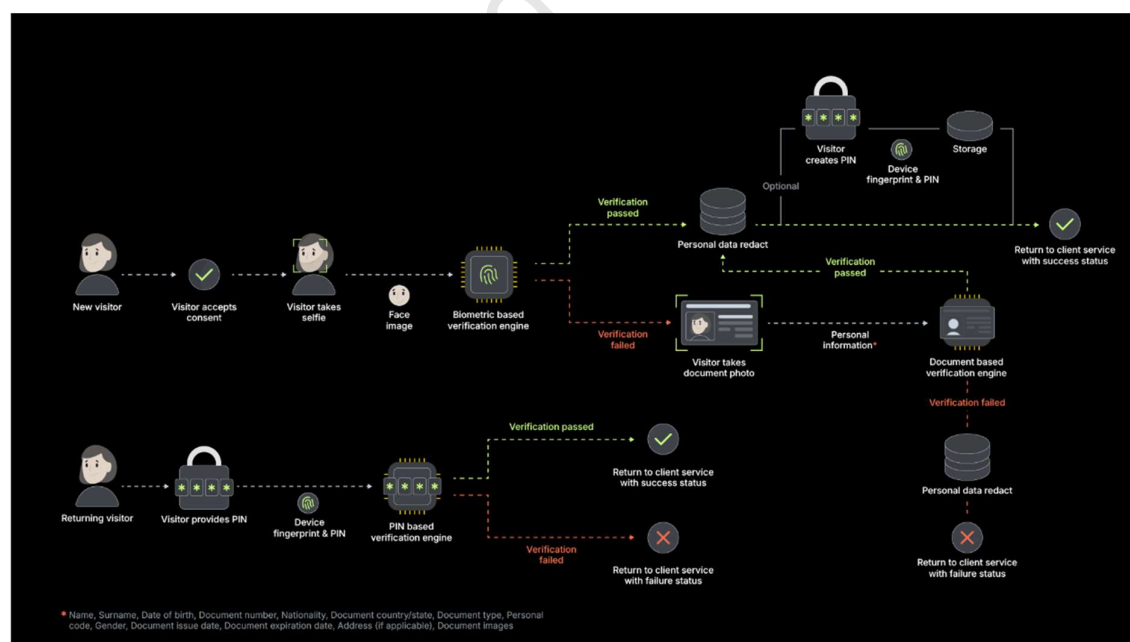
Client enforcement and optional parental consent

Parental consent and parental relationship verification is not in scope of Company's service. If parental consent is offered, first must be notified the minor and obtained their valid consent. Then notified parent, and assessed parental age status including verification of the parental relationship through a method reasonably calculated to do so and resist fraud.

Services in scope do not disclose the minor's content activity, contacts, personal attributes or settings to the parent beyond what the rules expressly require or other law strictly requires.

New York service workflow

The following process is part of this Practice Statement and defines the required Ondato and client integration. It documents the process design and production implementation.



Validation flow ensured by two parties (Client and Company) in close collaboration. Client is obliged to:

- Initial phase:
 - Client:
 - Determine covered platform and New York user status using reliable data;
 - investigate location concealment;
 - Explain method and data handling to the end-user;
 - offer certified methods and required non-ID route.
- Validation phase:
 - Ondato:
 - runs selected method with certified settings;
 - returns outcome and reason.
 - Client:
 - Recheck provided results;
 - Offer remaining qualifying methods or accessible appeal as applicable;
 - Test every condition of the narrow all-inconclusive presumption.
- Post validation phase:
 - Client:
 - Provide accessible appeal and, if offered, let minor choose whether to request parental consent.
- Continuously during all process:
 - Both sides:
 - Maintain minor protections;
 - Review non-ID/ID evidence in good faith;
 - Apply data deletion and minimal statutory records to every path;
 - monitor, investigate and correct status/consent changes.

New York outcome handling

The following names describe required logical states applicable to NY SAFE Act:

Logical state	Required treatment
ADULT_CONFIRMED	Method-confirmed adult. Client checks contrary knowledge before enabling restricted features.
MINOR	Actual-knowledge signal; apply minor protections, appeal and optional consent.

Logical state	Required treatment
INCONCLUSIVE	All requested data received; no detected circumvention; unable to determine status. Continue qualifying paths.
INCOMPLETE_OR_REFUSED	Requested input not provided. Never relabel as statutory inconclusive.
CIRCUMVENTION	Attack or false-data interference detected. No adult grant; investigate and count appropriately.
TECHNICAL_ERROR	No reliable result. Retry or alternative; no automatic pass.
ADULT_PRESUMED	Client-only decision after all defined conditions; not a successful method confirmation.
ADULT_ON_APPEAL	Client good-faith appeal reversal under requirements; preserve required decision evidence minimally.

The all-inconclusive path requires completion of every offered qualifying method, including one certified to the total accuracy minimum, with every result genuinely inconclusive and no actual knowledge of minor status.

The client verifies session/account binding and rejects tampered, replayed, cross-client or mismatched responses. The NY SAFE Act applied integration should return the least precise necessary status.

Compnay retains only legally required evidence, separating method outcomes from policy decisions.

Indicators of confidence

Company's Age assurance solution outputs:

- An age estimation (between 1 and 99 years) associated with an age range. The age range is the interval within which the client's age is estimated to fall. The age range is fixed for each given age and does not depend of the facial media process by our system. The age range is dependent on the model we use to estimate the age and configuration applicable to the Client.
- Age verification: when our system indicates that a user is above a certain age (given as a threshold), the system provides a confidence level (which can take two values: low or high) and a probability, which reflects the chance that the estimated age is above the given age threshold.

Inconclusive results are explicitly flagged and never default to pass or fail. Relying parties may ask to configure policy actions such as retry, assisted flow, or step-up verification. For each supported threshold Company's maintains deviation within ± 3 years, and false-accept/false-reject rates for under/over outcomes.

Under the New York profile, Company apply the narrow adult-presumption route defined in NY SAFE Act §700.4(b)(1)(ii), and after all required conditions are met, or reverse a decision through predefiend appeals. The Company forbidden to encode every inconclusive outcome as a pass.

Confidence outputs are calibrated against representative hold-out datasets. Outputs can be configured to meet multiple confidence indicators, including:

- an age estimate with a fixed model-dependent range;
- a binary pass/fail against a configured threshold with a confidence level, and
- attributes transmitted at varying precision levels (threshold-only, binary, or exact age where necessary);
- additional steps for validation (as document validation or validation against information in the registries) required according to the law or client demands

Binding process

Company's solution ensures binding of the age assurance result to the correct individual through the use of live facial captured (secured by liveness detection) and session integrity control:

- Liveness detection (Presentation Attack Detection, Injection Attack Detection): we use liveness detection algorithms to confirm that the source media is from a live person, captured in situ, and not a static photo, a video replay, a synthetic face (deepfake), etc.
- The facial media used for age estimation is session-linked to the requesting relying party session, ensuring that the result cannot be transferred or replayed across contexts. In keeping with privacy-by-design principles and where appropriate, the system performs age estimation without linking to a persistent identity or storing biometric templates—thus enabling binding without long-term data retention. Minimal or no persistent identifiers are used unless explicitly required by the relying party and lawful basis. Company's does not persist biometric templates unless explicitly configured and lawfully justified.
- Session integrity links captured media and/or the age proof to the relying party's current session; where suitable, stateless, session-bound tokens prevent reuse across sites or sessions. Capture artifacts are linked to the current session. Used Tokens are nontransferable between services or sessions.

Privacy and data protection

We adopt a privacy-centric and risk-based approach to personal data processing, fully aligned with the principles set out in ISO/IEC 27566-1, IEEE 2089 as well as with applicable data protection laws such as the EU General Data Protection Regulation (GDPR), Digital Operational Resilience Act (DORA), Network Information Security 2 Directive and relevant national frameworks and laws in jurisdictions where we operate.

For New York SAFE for Kids Act processing, the Company aligned with NY ACT requirements defined in in §700.7 part and the New York requirements in this statement govern.

Privacy Characteristics

Company's solution supports the following key privacy characteristics:

- **Data minimization:** Only the minimum amount of personally identifiable information (PII)—a single facial image or frame, and data from person identity document is processed to establish an age estimate.
- **Purpose limitation:** PII is collected solely for the purpose of age estimation, and we ensure that such data is not reused or repurposed unless explicitly authorized under a separate lawful basis. PII may be used for liveness detection purposes as well if the relying party decides to secure the age assurance process to ensure that the age assurance result is bound to the correct individual.

Data processed according to New York profile is used only to comply with the applicable provision. It is not reused for advertising, unrelated analytics, identity enrichment or model training. The narrower New York purpose limitation overrides any general allowance elsewhere in this statement for reuse under a separate legal basis.

- **Transparency and accountability:** Clear privacy notices and documentation are provided to users and relying parties, describing the processing activity, data retention, and user rights.
- **Security and integrity:** Robust technical and organizational measures are in place to prevent unauthorized access, tampering, or leakage of biometric data. Aligned, validated and certified according to ISO27001:2022 certification.

Minimal PII Processing

The system is designed to process, and store as minimum information as possible. In most configurations:

- A facial image is used only temporarily for real-time estimation and is discarded immediately after processing.

- No biometric template or identifiable record is stored unless explicitly required by the relying party and covered by an appropriate lawful basis (e.g. consent or contractual necessity).
- For the New York profile, persistent biometric templates and identifiable raw evidence are not retained merely because a client requests them or provides a general legal basis. Mandatory minimal compliance records are separated from raw evidence.

Purpose Limitation and Data Retention

PII processed for age estimation is:

- Used solely for that purpose;
- Not retained by default after the result is returned. Raw evidence is deleted immediately once the minimum necessary compliance purpose is completed, subject only to an applicable statutory exception. The required minimal records are retained separately under requirements §700.7(b) of NY SAFE Act.
- If authorized and applicable, any use of data for analytics, auditing, or model improvement is anonymized or aggregated and never linked to identifiable individuals without a separate legal basis.
- For New York profile data is not used for model improvement or unrelated analytics, including by suppliers. De-identification is permitted only with the and does not create permission for unrelated use.

Data Subject Rights Management

We uphold all applicable data subject rights under GDPR, DORA and NIS2 and other laws, including:

- Access: Where applicable, individuals can request confirmation of whether their data has been processed and, if so, obtain a copy.
- Rectification/Objection: Individuals can challenge results they believe to be based on inaccurate or incomplete data.
- Review of Automated Decisions: Where the age assurance result is used in a solely automated decision-making context, we support mechanisms for human review upon request.
- Erasure: Where applicable, individuals may request the deletion of their data.

New York users also receive the dedicated age-status appeal process, independently of any GDPR request process.

Security and Breach Management

We implement appropriate technical and organizational security measures aligned with ISO/IEC 27001 standard and eIDAS regulation. In the event of a personal data breach:

- We follow a structured incident management procedure defined and implemented in the company, including notification to supervisory authorities and affected individuals where required.
- All breaches are logged, assessed, and reviewed to ensure corrective actions and risk mitigation are applied.
- Our privacy practices are reviewed regularly as part of our ISMS management system and data protection impact assessments (DPIAs) are conducted prior to deployment or material changes, in accordance with Article 35 of GDPR.

New York data lifecycle requirements

New York profile data collected to comply with act requirements and must be limited to what is necessary, used only to comply with the applicable section, encrypted in transit and at rest, and retained only for the minimum necessary time before immediate deletion. A client instruction, general consent or a separate GDPR legal basis does not by itself permit another use of this compliance data.

Retain for at least five years, where applicable:

- the fact that a method was attempted;
- the method successfully confirming status;
- the determination date;
- the age status;
- and information necessary for applicable State or federal law or regulation.

Company retains monthly per-method totals for attempts, successful status determinations, adult determinations later corrected to minor, and adult-status denials due to circumvention.

Estimated age may be retained solely to determine status with valid user consent. Retained compliance data must not be used, alone or combined with other data, to identify an individual user. Company uses the least identifying operational linkage needed for the specified records and prohibit enrichment or cross-service identification.

The approved data map cover capture, liveness, OCR, supplier components, APIs, logs, support tools, temporary storage, replicas and backups. Separate minimal compliance records from raw evidence and implement deletion across all copies. If ordinary backup processes retain retrievable raw evidence after its purpose ends, the NY profile not enabled until an effective design is evidenced.

Ease of use

Company's Age Assurance solution is designed to provide maximum ease of use, with a particular focus on accessibility for users of all ages and capacities, including children and individuals with limited digital literacy. In line with the usability and inclusiveness principles outlined in ISO/IEC 27566-1, the system supports low-friction, intuitive interaction while maintaining reliability and regulatory compliance.

Key Ease-of-Use Features:

- **Fully Passive Interaction**
 - The system operates on a single selfie capture or picture capturing. And do not require typing, navigation, form-filling, or document upload.
 - There is no need for the user to understand or interpret the age assurance logic—the process runs automatically in the background.
- **No Personal Data Required**
 - Users are not required to enter personal details (e.g. name, birthdate, ID number), making the system especially accessible for young users who may not possess formal identity credentials.
- **Designed for Children and Adults**
 - The interface uses clear visual instructions, simple icons.
 - The selfie capture step is aligned with interaction patterns already familiar to most users, including children (e.g. taking a photo in an app).
- **Fast Response Time**
 - Age estimation results are typically delivered within seconds, minimizing user wait time and reducing dropout risk, especially for younger users with limited attention spans.
- **Device Compatibility and Accessibility**
 - The solution works on a wide range of smartphones, tablets, laptops and webcams, and can be embedded into native apps or web interfaces.
 - It is compatible with assistive technologies and accessible UI frameworks, depending on the relying party's implementation.
- **Re-usability**
 - For Authentication based on age verification results, we are providing solution, which allows clients to re-use initial age estimation and verification results for limited amount of time, by creating account with PIN. As additional security controls we are capturing device, used for age verification, fingerprint.

New York appeals and age status changes

Company's client offer a clear, conspicuous, accessible appeal, with at least one supporting-document option other than government identification. Evaluate submissions in good faith and send a written decision with reasons. Communicate a decision or request for further information within 10 business days of receipt, then decide expeditiously after receiving additional information. Company's client may reverse minor status through that appeal. Company support arrangements must allow these deadlines to be met.

Through provisioning services Company:

- investigates reports of false adult status and emerging circumvention;

- corrects validated false positives and improve detection.
- changes adult status to minor within 10 business days after actual knowledge is obtained.
- as a protective deployment control, disable affected restricted features promptly while that change is processed.

Users reaching 18 must have a route to a fresh qualifying age-assurance assessment; do not automatically promote an estimated age without the required assessment. [§700.4(d)]

Security measures

Company implementin Information Security Management System (hereinafter - ISMS), which is covering Company's services, development and maintenance processes. Defined ISMS is certified according to ISO27001 and eIDAS regulation requirements. Company ensure such Information Security principles as:

Confidentiality

- All image data captured for age estimation is transmitted over secure, encrypted channels;
- By default, the system processes data in memory and does not persistently store personally identifiable information;
- For New York processing, raw capture data must have the shortest necessary lifecycle, while statutory minimal records are segregated and retained under the approved schedule;
- Encryption at rest, backup handling and deletion across all copies must be evidenced before New York deployment;
- (PII) unless explicitly required by the relying party under a lawful basis.
- Access to any retained data is strictly controlled, audited, and limited to authorized personnel under role-based access policies.

Integrity

- Age estimation results are generated in a tamper-evident process, using signed requests and response tokens to
- prevent interception or result manipulation.

Availability

- The system is deployed across resilient infrastructure with load balancing, auto-scaling, and fallback support to maintain service continuity.
- We implement uptime monitoring and incident response protocols to ensure that the service remains accessible to relying parties without interruption.

Authentication and Session Security

- Facial data submitted for estimation is linked to a secured session token, ensuring the result is uniquely bound to the session in which the image was captured (as per binding requirements).

Resilience to Attacks

- The system incorporates liveness detection and anti-spoofing technology to defend against presentation attacks (e.g. photos, videos, or synthetic images).
- Regular penetration testing and vulnerability scans are conducted as part of our secure development lifecycle, and findings are tracked to remediation through our ISO 27001-aligned risk management process.

More details is provided in Company's publicly available whitepapers (Summary of control.pdf)

Human rights protections

Company commits to proportionate, inclusive, and transparent age assurance, through assurance of such functionality:

- **Accessibility & inclusion:**
 - simple interaction patterns;
 - options to select verification methods suited to user context;
 - ability for relying parties to integrate child-friendly UI.
- **Bias monitoring:**
 - ongoing review of outcomes across demographic groups and model improvement practices;
 - training data diversity is considered to mitigate unfair impacts.
- **Proportionate use:**
 - configurable thresholds help avoid undue restriction of access while meeting legal mandates.

New York transparency and user protection

Services provided accrodint to NY profile ensure explanation of the methods, requested data, purpose, use and deletion before collection.

Assess accuracy, attacks and user burden initially and periodically against commercially reasonable alternatives and adopt improvements reasonably and in good faith.

Document language/accessibility testing, release decisions, annual certification and consent-method are reviewed and documented.

Audit, certification, and review

Company's Age Assurance solution, practice statement, and development, maintenance and supporting processes are subject to:

- Internal audit;
- External audit;
- Third-party oversight;
- Penetration testing.

Such approach allows to ensure compliance with applicable Industries standards, applicable laws, including data protection law, and regulators requirements.

New York configuration and evidence records

The controlled deployment register identifies product/API/SDK/web releases, facial and liveness model versions, document verification engine and jurisdiction coverage, thresholds and buffers, confidence rules, fallback sequence, certification/report identifiers and validity dates, suppliers and infrastructure, deletion controls, minimal compliance records, and client integration ownership. The register map each deployed setting to its certification evidence.

New York approval and review

Product owner, Chief Technology Officer, Chief Information Security Officer, Data Protection Officer and Legal review the scope, certified configurations, data lifecycle, client integration and completed evidence before release. Certification-body acceptance and applicable client responsibilities are documented.

The evidence pack comprises the controlled configuration, certification and testing reports, data-flow and storage map, notices and alternative-method screens, redacted or synthetic API traces, appeals and optional consent/withdrawal records, deletion and restore-test results, and the completed validation register.

New York legal references

New York General Business Law Article 45 and 13 NYCRR Part 700. References throughout these amended sections are to Part 700. Final implementing rules: <https://ag.ny.gov/safe-for-kids-act-final-rule>

The New York Attorney General confirms an effective date of 25 January 2027: <https://ag.ny.gov/resources/individuals/consumer-issues/technology/protecting-children-online>. Sources reviewed on 23 September 2026.

Contact details

Role	Description	Person	Email	Phone
Product Owner	Overall accountability for service	Svajūnas Gaina	svajunas.gaina@ondato.com	

Chief Technology Officer	Technical solution and service development and maintenance	Gediminas Letulis	gediminas@ondato.com	
Chief Information Security Officer	Security best practices and controls implementation and control.	Dmitrij Olifer	dmitrij.olifer@ondato.com	+37065592092
Data Protection Officer	Data protection and Privacy, including Data Protection Impact Assessment, implementation and control.	Rūta Būčinskaitė	ruta@ondato.com	

Certified Summary