

ESCORTIFYS

GLOBAL VERIFICATION, IDENTITY & AGE- ASSURANCE POLICY

Document 6 | Pre-Publication Final Draft

Purpose

This Policy explains how Escortifys may verify Provider identity, adulthood, account control, and consent, and how Escortifys may perform age assurance for members or visitors where required by law, platform policy, content type, or access level.

Draft date: 23 August 2026 | Public effective date: [TO BE INSERTED AT LAUNCH]

Two different systems

Provider verification and viewer age assurance serve different purposes. Provider verification may need to establish who the Provider is and that the Provider is an adult controlling their own listing. Viewer age assurance should ordinarily establish only whether the viewer meets the required age threshold, without collecting identity information that is not necessary for that purpose.

Critical fraud rule

Deliberate identity-verification fraud - including knowingly using forged, stolen, synthetic, altered, borrowed, or another person's verification material - is a critical violation. Once confirmed for platform-enforcement purposes, permanent account termination is the default outcome.

Contents

1. Scope and relationship to other policies
2. Definitions
3. Verification principles
4. Adult-only baseline
5. Provider identity verification
6. Provider adulthood verification
7. Provider account-control verification
8. Consent and authority to publish
9. Viewer/member age assurance
10. Methods that may be used
11. Methods that may be insufficient
12. Multiple verification methods and accessibility
13. Government identification
14. Selfie, liveness, and facial matching
15. Facial age estimation and biometric processing
16. Digital identity, banking, card, mobile-network, and other signals
17. Data minimization and separation of functions
18. Verification vendors and processors
19. Storage and deletion of verification material
20. Verification results and badges
21. Re-verification
22. Age or identity uncertainty
23. Verification failures and disputes
24. Fraud, tampering, synthetic documents, and circumvention
25. Minors and attempted access
26. Jurisdiction-specific age thresholds
27. Geolocation and anti-circumvention
28. Automated decisions and human review
29. Security and access controls
30. Law enforcement, legal process, and preservation
31. No guarantee created by verification
32. Accessibility, fairness, and non-discrimination
33. Changes and contact
- Appendix A. Verification tiers
- Appendix B. Suggested retention model
- Appendix C. Internal legal and implementation notes - remove before publication

1. Scope and relationship to other policies

This Global Verification, Identity & Age-Assurance Policy applies to Provider verification, age assurance, identity checks, account-control checks, consent checks, re-verification, trust badges, verification disputes, and anti-fraud controls used by Escortifys.

It supplements the Terms of Service, Global Privacy Policy, Global Advertising & Listings Policy, Global Prohibited Content & Conduct Policy, Global Safety, Reporting & Takedown Policy, and any jurisdiction-specific addendum. If mandatory law or another Escortifys rule imposes a stricter standard, the stricter standard applies.

2. Definitions

Term	Meaning
Age assurance	Any method or process used to determine whether a person meets an age threshold, including age verification or age estimation.
Age verification	A process that confirms age or an age threshold from a source or credential associated with the person.
Age estimation	A process that estimates a person's age or age range, potentially using facial or other signals.
Identity verification	A process used to establish that a person is who they claim to be.
Provider verification	The combined process used to establish a Provider's adulthood, identity, account control, and authority to publish the listing.
Verification material	Documents, images, selfies, video/liveness captures, biometric templates, attributes, signals, credentials, tokens, or other information used in a verification process.
Verification result	The outcome of a check, such as verified adult, identity matched, failed, expired, or review required.

3. Verification principles

- **Necessity:** collect or generate verification information only where there is a legitimate verification, safety, fraud, or legal need.
- **Proportionality:** the intrusiveness of the method should match the risk and legal requirement.
- **Data minimization:** collect the least information reasonably needed to establish the required result.
- **Purpose limitation:** do not repurpose verification material for unrelated advertising, profiling, or surveillance.
- **Security:** protect verification information according to its sensitivity.
- **Accuracy and fairness:** use reliable methods and provide review for material errors where appropriate or required.
- **Storage limitation:** retain raw verification material only as long as needed for the verification purpose, dispute, fraud control, legal obligation, or legal hold.
- **Separation:** where practicable, store a verification result or token instead of retaining the underlying document or biometric material.

4. Adult-only baseline

Provider Listings are adult-only. A Provider must be at least 18 and must meet any higher age threshold required by the applicable jurisdiction or feature.

Escortifys may apply a 21+ threshold to some jurisdictions, content, features, or access tiers even where the general age of majority is 18.

A visitor or member may also be required to complete age assurance before accessing adult content or functionality where law, risk assessment, or platform policy requires it.

5. Provider identity verification

Before a Provider Listing is published, renewed, reactivated, or granted specified trust features, Escortifys may require reasonable proof that the person controlling the account is the person being advertised.

Verification may involve one or more of the following, depending on jurisdiction and risk:

- government-issued or other reliable identity document;
- selfie or live image matched to the identity credential;
- liveness or anti-spoofing check;
- reusable digital identity credential;
- telephone, email, device, or account-control confirmation;
- manual review where automated methods are uncertain;
- additional evidence where impersonation, exploitation, duplicate identity, or fraud indicators arise.

Escortifys may decline a method that is unverifiable, materially altered, expired, inconsistent, or inappropriate for the relevant jurisdiction.

6. Provider adulthood verification

Provider adulthood verification is separate from simply accepting a date of birth entered into a form. Escortifys may require documentary, digital-identity, age-estimation, or other reliable evidence sufficient to establish the required age threshold.

Where the law requires a stronger method, a self-declaration or contractual statement such as 'I am over 18' will not be treated as sufficient on its own.

7. Provider account-control verification

Because Escortifys uses a provider-controlled self-advertising model, verification must address control as well as identity.

- The Provider should be able to access, edit, pause, dispute, and delete the listing without permission from a third party.
- A manager, agency, partner, recruiter, employer, driver, studio, venue, or other person must not hold the Provider's credentials or control the listing under the baseline model.
- Escortifys may ask a Provider to complete a fresh login, contact-method challenge, liveness check, or manual confirmation when third-party control is suspected.
- Evidence that another person controls the Provider's documents, money, communications, or account may trigger a safety review.

8. Consent and authority to publish

Verification does not replace consent. A verified Provider must still have authority to publish every image, name, contact detail, statement, and other personal information included in the listing.

Where multiple adults appear in content, Escortifys may require separate proof of adulthood and consent for each depicted person or may prohibit the content under the applicable media rules.

Consent may be re-checked following an impersonation, stolen-image, non-consensual-content, trafficking, or account-control report.

9. Viewer/member age assurance

Where Escortifys must determine whether a visitor or member is old enough to access adult content or a restricted feature, the preferred design is to learn only the result needed for access - for example, that the person is 18+ - rather than their full identity or date of birth.

Age assurance may be required before content is displayed, not merely after the content has already been exposed, where applicable law requires pre-access protection.

10. Methods that may be used

Depending on law, availability, effectiveness, privacy impact, and user accessibility, Escortifys may use or support one or more of the following:

- photo-identification matching;
- reusable digital identity or age credentials;
- open-banking or bank-attribute confirmation that reveals only the necessary age threshold where available;
- credit-card age checks where the method reliably establishes the required adult threshold;
- mobile-network operator age status;
- facial age estimation with an appropriate challenge-age margin and privacy safeguards;
- email- or account-based age estimation where accepted by the relevant regulator and shown to be sufficiently effective;
- other privacy-preserving or regulator-recognized age-assurance methods that meet the applicable standard.

11. Methods that may be insufficient

The following may be insufficient on their own where a jurisdiction requires effective or highly effective age assurance:

- self-declaration of age;
- entering a date of birth without additional verification;
- a general '18+' warning or contractual restriction;
- a payment method that does not reliably require the user to be an adult;
- inference from browsing history, content preference, or prolonged use where the applicable regulator does not accept such inference as sufficient.

12. Multiple verification methods and accessibility

Escortifys should not force every user through the same method where a less intrusive, equally effective alternative is reasonably available. Where practicable and legally appropriate, more than one verification method should be offered.

Users who cannot use a particular method because of disability, lack of conventional documents, technical failure, regional availability, or another legitimate barrier may be offered a reasonable alternative, subject to fraud and legal controls.

13. Government identification

Government-issued identification may be used where proportionate and appropriate, but Escortifys does not treat government ID as the only acceptable age-assurance method for viewers where another reliable method is available and permitted.

When government ID is used, collection should be limited to what is needed. Information such as document number, full address, nationality, or other fields should not be retained merely because they appear on the document if they are unnecessary for the verification purpose.

Where technically feasible, unnecessary fields should be masked, discarded, or processed by a verification provider without being retained by Escortifys.

14. Selfie, liveness, and facial matching

A selfie, live image, or liveness check may be used to determine whether the person presenting an identity credential is the same person shown on that credential and to reduce spoofing.

Such material is sensitive. It must not be used for marketing, public display, facial-search databases, or unrelated surveillance.

Liveness or facial matching should be tested for reliability and should permit human review of material errors where appropriate.

15. Facial age estimation and biometric processing

Facial age estimation may be used only where legally permitted, reasonably effective, proportionate, and supported by appropriate privacy and security measures.

Where a process creates or uses a biometric template or biometric information for automated verification or identification, Escortifys will treat that information as highly sensitive and apply enhanced safeguards.

- Use a challenge-age or safety-margin approach where necessary to reduce the risk that a minor close to the threshold is incorrectly treated as an adult.
- Do not use biometric information collected for verification to infer health, ethnicity, attractiveness, sexual orientation, or unrelated characteristics.
- Delete or de-identify biometric templates when no longer necessary, subject to lawful preservation requirements.
- Assess vendor accuracy, bias, spoof resistance, security, and deletion practices before deployment and periodically afterward.

16. Digital identity, banking, card, mobile-network, and other signals

Escortifys may use age attributes supplied by a trusted digital identity provider, bank, card issuer, mobile operator, or other reliable source where the method is legally permitted and appropriate.

Where possible, the source should return only the necessary result - such as 'over 18' - rather than the person's full date of birth, account details, financial history, or identity.

A successful card payment for an Escortifys platform product does not automatically prove adulthood unless the specific age-check method itself reliably establishes the relevant threshold.

17. Data minimization and separation of functions

Verification systems should be designed so that identity verification, age assurance, fraud prevention, public profile display, advertising, analytics, and moderation do not automatically share all underlying verification data.

- Public profiles should display a verification status or badge, not raw identity documents.
- Moderation personnel should ordinarily see only what is necessary for the moderation or verification task.
- Advertising and analytics systems should not receive raw identity documents, verification selfies, liveness media, biometric templates, or exact birth dates merely because those data exist.
- Viewer age-assurance records should, where practicable, be unlinkable from adult-content browsing history beyond what is necessary to maintain lawful access control and security.

18. Verification vendors and processors

Escortifys may use specialized third-party verification providers. Before deployment, Escortifys should conduct due diligence proportionate to the sensitivity of the data and the legal risk.

- where the vendor processes data and in which countries;
- which documents, images, templates, or attributes it collects;
- whether it creates biometric templates or facial embeddings;
- retention and deletion periods;
- subprocessors and cross-border transfers;
- security controls and breach history;
- accuracy, bias, challenge-age, liveness, and spoof-resistance testing;
- whether the vendor uses data to train models or for unrelated purposes;
- whether contract terms prohibit unauthorized secondary use and require deletion/return.

19. Storage and deletion of verification material

Escortifys' preferred architecture is to retain the minimum verification result necessary for account administration and to avoid retaining raw identity or biometric material when a reliable verification token or result is sufficient.

Unless a different period is required by law, fraud investigation, dispute, or legal hold, raw identity documents and raw verification selfies should ordinarily be deleted or rendered inaccessible promptly after the verification decision and should not become a permanent account archive.

The final production retention periods must match the Privacy Policy, vendor contracts, technical implementation, and jurisdiction-specific law.

20. Verification results and badges

A badge or verification status means only that the checks expressly described by Escortifys were completed at a particular time. It does not guarantee safety, legality, health, character, service quality, availability, or future conduct.

Users may not copy, manufacture, alter, or falsely display Escortifys verification badges.

21. Re-verification

Escortifys may require re-verification when reasonably necessary, including after:

- material changes to identity, profile ownership, contact methods, or listing control;
- expiration or revocation of a relevant credential;
- a material impersonation, trafficking, coercion, stolen-image, or account-control report;
- suspected account sale, transfer, rental, or takeover;
- suspicious login or anti-fraud signals;
- a jurisdiction change that changes the required age or verification standard;
- a significant period of inactivity or an appropriate scheduled verification interval.

22. Age or identity uncertainty

Where reliable verification cannot be completed, Escortifys may refuse publication or deny access to a restricted feature. The Platform is not required to resolve uncertainty in favour of publication or adult access.

Where an automated method produces a borderline or uncertain result, Escortifys may request an alternative method or human review rather than treating the person as verified.

23. Verification failures and disputes

A user may dispute an eligible verification failure, mistaken identity, or re-verification decision by using the designated verification-dispute process.

Escortifys may request limited additional information necessary to resolve the dispute. A dispute does not entitle the account to remain public or access age-restricted content while verification is unresolved.

24. Fraud, tampering, synthetic documents, and circumvention

- forged, altered, stolen, borrowed, synthetic, or unlawfully obtained identity documents;
- AI-generated or manipulated selfies, liveness recordings, faces, documents, or age evidence;
- use of another person's verification session, token, account, phone, card, bank attribute, or digital identity;
- selling, renting, lending, or transferring a verified account;
- using false location, proxy identity, alternate account, or technical measures for the purpose of defeating a known age or verification restriction.

Deliberate identity-verification fraud, once confirmed for platform-enforcement purposes, carries permanent account termination as the default consequence, along with reasonable anti-circumvention measures where legally permitted.

25. Minors and attempted access

If Escortifys determines that a person is below the required age for a Provider account or adult feature, access or publication will be denied. Escortifys may retain a limited anti-abuse record where legally permitted and necessary to prevent immediate re-registration or protect children.

Escortifys should not retain unnecessary sensitive information about a minor merely to prove that access was denied.

26. Jurisdiction-specific age thresholds

Age thresholds and required assurance methods vary. Escortifys may apply different rules based on the user's location, Provider location, content type, feature, service classification, or another legally relevant connection.

A globally displayed '18+' notice does not replace jurisdiction-specific age-assurance duties.

27. Geolocation and anti-circumvention

Escortifys may use coarse location, IP intelligence, jurisdiction settings, device or security signals, or other proportionate tools to determine which age-assurance rule applies and to reduce deliberate circumvention.

Privacy tools are not prohibited merely because they are privacy tools. Prohibited conduct is intentional evasion of a known age, verification, or jurisdiction restriction.

Any use of device telemetry, persistent identifiers, VPN detection, or similar anti-circumvention tools must comply with the Privacy Policy and applicable law.

28. Automated decisions and human review

Automated verification, fraud scoring, facial matching, age estimation, or liveness results may assist a decision but are not infallible.

Where a decision has a significant adverse effect and applicable law or platform policy requires review, Escortifys should provide an appropriate human-review or alternative-verification pathway.

A risk score or failed automated match is not proof of criminal conduct.

29. Security and access controls

Verification information requires safeguards appropriate to its sensitivity. Measures may include encryption, restricted-role access, segregation from public systems, audit logging, secure transmission, vendor controls, retention automation, and deletion verification.

Exact technical architecture is confidential and may change. The public Policy describes principles, not a security blueprint.

30. Law enforcement, legal process, and preservation

Verification information is not automatically available to government authorities. Requests for non-public verification information are handled under the Law Enforcement & Government Requests Policy and applicable law.

Escortifys may preserve verification records when legally required or reasonably necessary for a legal hold, critical safety matter, fraud dispute, or lawful process. Preservation does not itself authorize disclosure.

31. No guarantee created by verification

Verification confirms only the limited attributes actually checked. Escortifys does not warrant that a verified user is safe, honest, lawful, healthy, compatible, free of criminal history, or suitable for any offline interaction.

32. Accessibility, fairness, and non-discrimination

Verification systems should be designed and tested to reduce unfair exclusion, discriminatory error, and inaccessible verification barriers.

- Where reasonable, provide alternative verification methods for users who cannot complete a particular method.
- Do not use verification technology to infer protected characteristics that are unnecessary to the verification purpose.
- Monitor material error rates and complaints across relevant user groups where lawful and practicable.
- Do not treat a technical verification failure as proof of fraud without supporting evidence.

33. Changes and contact

Escortifys may update this Policy to reflect legal developments, regulator guidance, vendor changes, security threats, technical improvements, content changes, or geographic expansion.

Platform: Escortifys.

Verification support / disputes: [TO BE INSERTED]

Privacy contact: [TO BE INSERTED]

Legal notices: [TO BE INSERTED]

Operator, controller, merchant, service-address, or similar particulars are disclosed where applicable law requires proactive disclosure and may otherwise be provided in response to an appropriate request.

Appendix A - Verification tiers

Tier	Verification purpose	Typical effect
Tier 0 - public visitor	No identity verification by default; age gate or jurisdiction control may apply	No public posting privileges
Tier 1 - member / restricted viewer	Age assurance as required by law or content risk; identity should not be collected unless necessary	Access to age-restricted features only after required threshold is established
Tier 2 - Provider	Identity + adulthood + account control + consent/authority	Required before Provider Listing publication
Tier 3 - elevated-risk / re-verification	Fresh or enhanced verification after risk signal, dispute, account change, or jurisdiction change	May include human review or alternative evidence

Appendix B - Suggested retention model

Data type	Suggested baseline	Control
Raw Provider ID document	Delete promptly after final verification decision; target ordinarily within 30 days unless fraud, dispute, legal duty, or hold requires longer	Do not use as permanent profile archive
Raw verification selfie / liveness media	Delete promptly after decision; target ordinarily within 30 days unless needed for dispute/fraud/legal hold	Keep separate from public profile media
Biometric template / facial embedding	Delete as soon as no longer necessary; prefer vendor-side transient processing	Treat as highly sensitive
Verification result / token	Retain while reasonably needed to maintain verification status, prevent fraud, or meet legal/accountability requirements	Prefer threshold/result over raw evidence
Failed-verification anti-abuse record	Short, proportionate retention where necessary to prevent immediate circumvention	Avoid retaining unnecessary raw documents
Audit log	Retain according to Privacy Policy and security/accountability schedule	Log access, decision, method, vendor, and relevant timestamps

Appendix C - Internal legal and implementation notes

INTERNAL - REMOVE BEFORE PUBLIC POSTING

This appendix records current-law research, project assumptions, and implementation gates. It should not appear in the final public web version.

C1. Project-record basis

- Historical planning describes Escortify as a global adult-classifieds platform in which verified escorts can create premium listings, with location-based filtering and VIP placement. That material is treated as historical architecture only and does not establish that every older feature remains current.
- Current project planning includes static verification and anti-bot explainers and contemplates verification-first posting, age acknowledgment, consent logging, terms/privacy acceptance tracking, audit logs, and legal-review gating.
- Current project records confirm that live workflows such as login/register/VIP gating, review submission, provider-safety reports, payments, messaging, booking/contact exchange, submissions, and admin actions were still placeholder-only at the cited development stage.
- Document 5 establishes permanent termination by default for confirmed deliberate identity-verification fraud and retains the existing staff/moderator access design unchanged for now.

C2. Canada - privacy and biometrics

The Office of the Privacy Commissioner of Canada issued private-sector biometric guidance in August 2025. It treats biometric information as often sensitive because it is stable, difficult to change, and closely linked to identity. The OPC advises organizations to establish a legitimate need, effectiveness, minimal intrusiveness, proportionality, appropriate consent, purpose limitation, limited retention, and strong safeguards.

Implementation consequence: if Escortify or a vendor creates facial templates, embeddings, liveness data, or other biometric information, complete a privacy impact/risk assessment, document necessity and alternatives, obtain appropriate consent where required, restrict secondary use, and delete the material when no longer necessary.

C3. European Union / EEA - GDPR and EDPB age-assurance principles

The European Data Protection Board's Statement 1/2025 on Age Assurance emphasizes lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, confidentiality, integrity, accountability, data protection by design/default, and proportionality. Age assurance should not become a general identity system where a simple threshold result is sufficient.

Implementation consequence: design EU age assurance around attribute disclosure and unlinkability where feasible; avoid collecting full identity or date of birth merely to establish an 18+ result; complete required DPIA/legal-basis work before high-risk biometric processing.

C4. United Kingdom - highly effective age assurance

Ofcom's Online Safety Act guidance identifies methods capable of being highly effective, including photo-ID matching, open banking, facial age estimation, mobile-network operator checks, credit-card checks, digital identity services, and certain email-based estimation. Self-declaration, an unverified date of birth, general contractual warnings, and payment methods that do not require adulthood are not capable of being highly effective.

Ofcom's July 2026 age-assurance report reiterates that providers remain responsible for effectiveness even when age assurance is outsourced and urges vendor due diligence and compliance with privacy/data-protection obligations. Ofcom is actively enforcing the regime and has issued material penalties and confirmation decisions against adult services.

Implementation consequence: if Escortify falls within the relevant UK duties because of content/service design, pornographic content must not be exposed before/during the age check, and the full end-to-end process must be technically accurate, robust, reliable, and fair.

C5. Australia - appropriate age assurance

Australia's Age-Restricted Material Codes are now in force across relevant service categories. eSafety states that appropriate age assurance can include photo-ID matching, facial age estimation, credit-card checks, digital identity systems, and other methods, but emphasizes privacy minimization and says services should offer more than one method where appropriate and should not rely on government-issued ID as the sole method.

The OAIC's March 2026 guidance states that biometric information and biometric templates used for automated verification/identification are sensitive information and should receive enhanced safeguards, necessity assessment, lawful/fair collection, and secure destruction or de-identification when no longer needed.

Implementation consequence: Australian launch should offer a privacy-preserving alternative to government ID where required by the applicable code/standard and should document anti-circumvention, fairness, privacy, and vendor controls.

C6. United States - state-specific age-verification laws

United States age-verification obligations vary materially by state and service type. In *Free Speech Coalition, Inc. v. Paxton*, 606 U.S. ____ (2025), the U.S. Supreme Court upheld Texas's age-verification requirement for covered websites containing a substantial portion of material obscene to minors. That decision does not create one nationwide implementation rule for every adult platform.

Implementation consequence: maintain a state launch matrix and assess each state's threshold, covered-content definition, acceptable verification methods, privacy/data-retention restrictions, enforcement mechanism, and constitutional litigation status before enabling adult content in that state.

C7. Vendor-selection rule

Do not select a verification vendor solely because it integrates quickly. The vendor must be evaluated for legal coverage, data location, biometric processing, security, liveness/spoof resistance, error rates, bias/fairness, challenge-age controls, deletion, subprocessors, breach history, secondary-use/training terms, and ability to return only a threshold result where appropriate.

C8. Preferred architecture

- Provider verification: use a specialized third-party verifier where practical; Escortifys should receive identity/adult/account-control results and minimal evidence necessary to manage disputes rather than store permanent copies of raw IDs.
- Viewer age assurance: prefer methods that return only an age-threshold result and do not reveal identity or exact date of birth to Escortifys.
- Raw ID/selfie/liveness: target deletion ordinarily within 30 days after final decision unless an active fraud dispute, legal duty, or hold justifies longer retention.
- Biometric templates: prefer transient vendor-side processing and prompt deletion; do not retain for marketing, profiling, search, or unrelated fraud databases.
- Badge: expose only status and verification date/expiry where useful; never expose raw verification evidence.
- Re-verification: trigger on material account-control changes, serious safety reports, credential expiry, account transfer signals, or jurisdiction changes.
- Human review: maintain a path for borderline age estimates, false non-matches, accessibility barriers, and material adverse verification decisions.

C9. Launch questions still open

- Final provider-verification vendor and exact data flow.
- Whether Escortifys itself will ever receive raw government ID or whether the vendor alone will process it.
- Whether any facial age estimation or biometric template is used.
- Whether viewer age assurance is required globally or only in specific jurisdictions/content areas.
- Final public media standard and whether any content legally characterized as pornography will be permitted.
- Exact age threshold by jurisdiction and feature, including any 21+ rule.
- Final member/VIP access model and whether age assurance can be reused across sessions.
- Final verification-dispute contact and service-level workflow.

C10. Official sources reviewed

- Office of the Privacy Commissioner of Canada, Biometrics and privacy; Biometrics quick tips for businesses (2025).
- European Data Protection Board, Statement 1/2025 on Age Assurance (12 February 2025).
- Ofcom, Guidance on Highly Effective Age Assurance; Quick Guide to Implementing Highly Effective Age Assurance; Use of Age Assurance Report 2026 (27 July 2026); 2026 enforcement programme materials.
- eSafety Commissioner, Age-Restricted Material Codes and current FAQ on accessing online porn and adult content (2026).
- Office of the Australian Information Commissioner, Privacy guidance on age assurance technologies (March 2026).
- Supreme Court of the United States, Free Speech Coalition, Inc. v. Paxton, 606 U.S. ____ (2025).

Publication status

Document 6 is substantively complete as a global baseline. Before public posting, finalize the verification vendor/data flow, viewer age-assurance scope, public media standard, jurisdiction matrix, retention automation, dispute route, and any proactive identity/controller disclosures required by applicable law. Then remove Appendix C.