

ESCORTIFYS

GLOBAL COOKIE & TRACKING TECHNOLOGIES POLICY

Document 8 | Pre-Publication Final Draft

Purpose

This Policy explains how Escortifys may use cookies and similar technologies, how those technologies are categorized, when consent or another choice is required, how users can manage preferences, and the heightened restrictions that apply because Escortifys may handle sensitive adult-content, identity, verification, location, and safety-related information.

Draft date: 28 August 2026 | Public effective date: [TO BE INSERTED AT LAUNCH]

Sensitive-site rule

Escortifys should not permit third-party advertising pixels, cross-site behavioural tracking, or unrelated analytics to receive information from identity-verification pages, age-assurance flows, private safety/fraud systems, legal-reporting forms, private communications, or other pages whose very use may reveal highly sensitive information.

No fictional cookie list

The public cookie inventory must reflect the production site actually deployed. This draft therefore does not invent cookie names, domains, vendors, or lifetimes. Before publication, Escortifys must complete a technical scan and insert or link a current live inventory.

Contents

1. Scope and relationship to the Privacy Policy
2. What cookies and similar technologies are
3. Technologies covered by this Policy
4. Core principles
5. Strictly necessary technologies
6. Preference and functionality technologies
7. Analytics and performance technologies
8. Advertising and measurement technologies
9. Security, fraud-prevention, and anti-bot technologies
10. Age-assurance and verification technologies
11. Local storage, session storage, and similar browser storage
12. Tracking pixels, web beacons, and conversion tags
13. Device fingerprinting and probabilistic identifiers
14. Embedded third-party content
15. Email tracking
16. First-party and third-party technologies
17. Sensitive-data restrictions
18. Consent and lawful choice
19. Cookie banner design
20. Rejecting non-essential technologies
21. Withdrawing or changing consent
22. Consent records
23. Browser signals and Global Privacy Control
24. Do Not Track
25. Analytics minimization
26. Behavioural advertising restrictions
27. Children and underage users
28. Retention and expiry
29. Third-party vendors and due diligence
30. Cross-border processing
31. Security
32. Jurisdiction-specific rules
33. Cookie settings and browser controls
34. Changes and contact
- Appendix A. Live cookie inventory requirements
- Appendix B. Consent-banner standard
- Appendix C. Internal legal and implementation notes - remove before publication

1. Scope and relationship to the Privacy Policy

This Global Cookie & Tracking Technologies Policy applies to escortifys.com, approved subdomains, web interfaces, and other digital services that expressly incorporate it. It covers technologies that store information on, access information from, recognize, or observe a browser, device, session, account, or interaction.

This Policy supplements the Global Privacy Policy. The Privacy Policy governs the broader collection, use, disclosure, retention, protection, and rights framework for personal information. Where this Policy and mandatory law impose a stricter requirement for a particular tracking technology, the stricter requirement applies.

2. What cookies and similar technologies are

A cookie is a small data file or identifier stored by a website or related service on a browser or device. Similar technologies can perform comparable functions without using a traditional cookie.

Some technologies are necessary to make a service work securely. Others remember preferences, measure performance, prevent abuse, support age or identity controls, attribute advertising, or track activity across pages, sessions, devices, or services.

3. Technologies covered by this Policy

- HTTP cookies and similar browser cookies;
- local storage, session storage, IndexedDB, and comparable browser storage;
- tracking pixels, web beacons, conversion tags, and transparent image requests;
- software-development-kit identifiers if an app or embedded service is later introduced;
- device or browser identifiers, advertising identifiers, and pseudonymous IDs;
- device fingerprinting or probabilistic identification techniques;
- server-side tagging or conversion APIs where browser or user activity is transmitted to a third party;
- embedded third-party media, maps, CAPTCHA/anti-bot tools, payment widgets, verification tools, or social content that can read or set device information;
- link-decoration, campaign identifiers, referral tags, and similar measurement technologies.

4. Core principles

- **Necessity:** do not deploy a technology merely because a vendor offers it.
- **Purpose limitation:** define what the technology does and do not quietly repurpose it.
- **Data minimization:** collect the least information reasonably needed for the approved purpose.
- **Choice:** where consent or opt-out rights apply, make the choice real, understandable, and technically effective.
- **No dark patterns:** do not pressure users into accepting tracking through misleading colour, wording, button hierarchy, or obstructive controls.
- **Sensitive-data protection:** avoid third-party tracking where page context or transmitted fields may reveal sexual life, sexual orientation, precise location, identity verification, legal complaints, safety reports, or similarly sensitive information.
- **Vendor accountability:** understand what a third party receives, where it sends data, what it does with the data, and how long it keeps it.
- **Auditability:** maintain a current inventory and periodically verify that deployed technologies match disclosed technologies.

5. Strictly necessary technologies

Strictly necessary technologies are used only where reasonably required to provide a service requested by the user, maintain security, authenticate a session, remember a privacy choice, prevent immediate abuse, balance load, maintain checkout integrity, or perform another function that cannot reasonably be provided without the technology.

Examples may include session authentication, CSRF protection, security routing, consent-preference storage, anti-fraud session controls, and limited age-gate state where legally and technically necessary.

A technology is not strictly necessary merely because it is useful to Escortifys, improves marketing, measures audience size, or increases advertising revenue.

6. Preference and functionality technologies

Preference technologies may remember language, region, interface settings, accessibility preferences, display choices, or other user-requested settings. Where these technologies are not strictly necessary, Escortifys will obtain the consent or provide the choice required by applicable law.

7. Analytics and performance technologies

Analytics technologies may be used to understand aggregate traffic, performance, errors, page usage, search quality, feature adoption, and service reliability after privacy review.

Escortifys' preferred analytics model is first-party or privacy-preserving measurement that minimizes identifiers, does not collect sensitive form fields, avoids creating cross-site profiles, and reports aggregate metrics wherever reasonably possible.

Non-essential analytics will not be activated before consent in jurisdictions that require prior consent.

8. Advertising and measurement technologies

If Escortifys uses advertising, affiliate, attribution, conversion, or campaign-measurement technologies, those technologies must be separately reviewed. They must not receive sensitive information merely because a user visits or interacts with an adult-content page.

Cross-context or cross-site behavioural advertising is subject to enhanced restrictions and may be disabled entirely in jurisdictions, page categories, or account areas where the legal or privacy risk is unacceptable.

9. Security, fraud-prevention, and anti-bot technologies

Escortifys may use cookies or similar technologies to detect bots, rate-limit abuse, protect login or verification flows, detect account compromise, prevent payment fraud, identify repeated policy evasion, or protect infrastructure.

Security and anti-bot technologies may be treated as necessary where their use is genuinely required for security or service integrity. They must not be used as a pretext for unrelated advertising or profiling.

Exact anti-bot rules, risk thresholds, fingerprints, and abuse-detection logic are confidential and are not disclosed in this public Policy.

10. Age-assurance and verification technologies

Age-assurance or identity-verification providers may use device storage, session identifiers, liveness signals, fraud indicators, or other technologies necessary to complete a verification process.

Those technologies are governed by the Verification, Identity & Age-Assurance Policy and Privacy Policy in addition to this Policy. Verification-related device information must not be repurposed for unrelated advertising or behavioural profiling.

11. Local storage, session storage, and similar browser storage

Local storage and similar browser technologies can retain information longer or in different ways than traditional cookies. Escortifys will classify them by purpose rather than pretending that a non-cookie storage mechanism escapes cookie or privacy rules.

Where a consent rule applies to storing or accessing information on a user's device, using local storage, SDK storage, pixels, or a similar mechanism instead of a traditional cookie does not avoid that requirement.

12. Tracking pixels, web beacons, and conversion tags

A tracking pixel or web beacon can transmit information to Escortifys or a third party when a page, image, advertisement, or message is loaded. The transmitted information may include URL, IP address, device/browser information, identifiers, page activity, or other event data.

Escortifys must configure pixels so that sensitive information is not unintentionally included in URLs, event names, form fields, custom parameters, or page titles.

Third-party pixels should not be deployed on verification, identity, age-assurance, private safety/fraud, legal-reporting, private-message, or other highly sensitive flows unless a documented necessity, lawful basis, technical minimization, and applicable consent requirement have been satisfied.

13. Device fingerprinting and probabilistic identifiers

Device fingerprinting can combine browser, device, network, and configuration signals to recognize or distinguish a device. Escortifys may use narrowly tailored fingerprinting for security, anti-fraud, bot detection, age-assurance integrity, or serious abuse prevention where lawful and proportionate.

Fingerprinting must not be used to secretly recreate advertising profiles after a user rejects non-essential tracking or to defeat deletion, consent withdrawal, or opt-out choices.

14. Embedded third-party content

Embedded videos, maps, CAPTCHA tools, social content, payment widgets, verification tools, or other third-party components may cause the third party to receive device or usage information.

Escortifys should block or delay non-essential embedded content until the required consent is obtained where applicable. Where a third-party component is strictly necessary to provide a requested function, its data collection must still be minimized and disclosed.

15. Email tracking

Escortifys may use limited delivery, security, or campaign-measurement signals in operational or marketing email where lawful. Tracking pixels or link measurement in email must not be used to infer sensitive sexual interests, exact location, or other highly sensitive characteristics without a lawful and proportionate basis.

Marketing communications remain subject to applicable anti-spam, direct-marketing, consent, and unsubscribe rules independently of this Cookie Policy.

16. First-party and third-party technologies

First-party technologies are set or controlled by Escortifys for Escortifys purposes. Third-party technologies involve another provider that may receive device or activity information.

A technology being 'third party' does not automatically make it unlawful, and a technology being 'first party' does not automatically make it privacy-safe. Escortifys evaluates the purpose, data, recipients, retention, user choice, and legal requirements.

17. Sensitive-data restrictions

Because context on Escortifys can itself reveal highly sensitive information, Escortifys applies a heightened restriction to tracking technologies.

- Do not transmit government ID, verification selfies, liveness media, biometric templates, or exact date of birth to analytics or advertising systems.

- Do not transmit private Provider Safety Reports, restricted fraud/safety records, reporter identity, legal complaints, or private moderation notes to advertising or general analytics providers.
- Do not transmit private-message content or contact-form text through analytics event parameters.
- Do not use page URLs, titles, search queries, listing categories, or profile attributes as advertising-event parameters where they could reveal sexual life, sexual orientation, sensitive identity, or another protected characteristic.
- Do not send precise geolocation to a third-party tracker unless the feature genuinely requires it, the processing is lawful, and the user has made the required choice.
- Do not create advertising audiences from verification failure, trafficking reports, safety complaints, law-enforcement requests, or other safety/legal events.

18. Consent and lawful choice

Where applicable law requires consent before a non-essential technology is stored or accessed, Escortifys will not activate that technology until valid consent has been obtained.

Consent must be specific enough to identify the relevant purposes, informed, freely given where that standard applies, and expressed through a positive action. Merely continuing to browse is not treated as consent where the law requires an affirmative choice.

Where applicable law permits another form of consent or opt-out for a particular practice, Escortifys may use that model only if the required transparency, control, sensitivity, and other legal conditions are satisfied.

19. Cookie banner design

Where a consent banner is required, it should present an honest choice rather than a persuasion exercise.

- Do not set non-essential technologies before the required consent.
- Provide a clear way to accept and reject non-essential technologies.
- Do not make 'Accept All' materially more prominent than the corresponding rejection choice where such design would undermine valid consent.
- Do not use pre-ticked non-essential categories.
- Do not make rejection take substantially more steps than acceptance.
- Explain categories and purposes in plain language and provide access to the current cookie inventory.
- Allow granular choices where required or appropriate.
- Record the user's choice and avoid repeatedly asking without a legitimate reason.

20. Rejecting non-essential technologies

Rejecting non-essential technologies should not disable the core service merely to coerce consent. Features that technically depend on a rejected optional technology may be unavailable if no privacy-preserving alternative can reasonably provide them, but the site must not falsely label marketing or general analytics as essential.

21. Withdrawing or changing consent

Users should be able to reopen Cookie Settings and change or withdraw non-essential consent as easily as reasonably practicable. Withdrawal applies prospectively and should prevent new non-essential tracking after the choice takes effect.

Withdrawing consent does not necessarily delete information already lawfully collected. Deletion and other privacy rights are governed by the Privacy Policy and applicable law.

22. Consent records

Where consent must be demonstrated, Escortifys may maintain a limited record of the consent state, timestamp, policy/banner version, jurisdiction or applicable rule set, and relevant categories. The consent record itself should not become a behavioural-tracking profile.

23. Browser signals and Global Privacy Control

Where applicable law requires recognition of an opt-out preference signal, including a qualifying Global Privacy Control or similar signal, Escortifys will process the signal as required for the relevant browser, device, profile, or processing activity.

A signal that legally opts a user out of sale, sharing, targeted advertising, or another covered activity will not be ignored merely because Escortifys also provides a site-level preference control.

24. Do Not Track

Browser 'Do Not Track' signals do not have one uniform legal meaning worldwide. Escortifys will respond to browser or device signals where applicable law requires a response. This section does not limit recognition of Global Privacy Control or another legally recognized opt-out preference signal.

25. Analytics minimization

Escortifys' analytics strategy is to measure approved aggregate or operational metrics after privacy review and to avoid leaking personal or sensitive information.

- Avoid full URLs containing account IDs, search terms, contact data, or sensitive profile attributes where not necessary.
- Avoid keystroke, form-field, password, message, or identity-document capture.
- Use IP truncation, pseudonymization, sampling, short retention, or first-party processing where appropriate.
- Do not enable session replay on sensitive forms or account areas without a specific documented review.
- Do not use analytics merely because it is bundled with hosting, advertising, or another vendor product.

26. Behavioural advertising restrictions

Escortifys does not treat behavioural advertising as necessary to use the Platform. If behavioural or cross-context advertising is introduced, it requires separate privacy/legal review before deployment.

Sensitive data and sensitive page context must not be used to build advertising profiles or audiences. In jurisdictions that require opt-in consent, such tracking will remain off until consent. In jurisdictions that provide opt-out rights, recognized opt-out controls and preference signals will be honoured where applicable.

27. Children and underage users

Escortifys adult areas are not directed to children. Escortifys does not intentionally use behavioural advertising or non-essential profiling to target minors.

If an age-assurance process indicates that a person is below the applicable threshold, optional advertising or analytics technologies should not be activated as a consequence of that failed access attempt merely to monetize or profile the minor.

28. Retention and expiry

Cookie and identifier lifetimes should be no longer than reasonably necessary for the stated purpose. Session technologies should expire when their purpose ends where feasible. Persistent technologies must have a documented retention or expiry rationale.

The live cookie inventory should state each technology's duration or retention period where reasonably knowable. Indefinite tracking identifiers require specific justification and should be avoided.

29. Third-party vendors and due diligence

Before deploying a third-party tracker, Escortifys should understand and document:

- the specific data collected or accessed;
- the purpose for which Escortifys uses the technology;
- whether the vendor uses data for its own purposes;
- whether the vendor combines data across customers or services;
- whether sensitive data could be inferred from page context or parameters;
- the countries in which data is processed;
- retention and deletion rules;
- subprocessors;
- security controls and incident history;
- available consent, opt-out, restricted-data, server-side, or privacy-preserving configuration;
- whether the vendor contract prohibits sending sensitive categories and whether Escortifys' configuration complies with those restrictions.

30. Cross-border processing

A tracking vendor may process information outside the user's country. Cross-border processing is governed by the Privacy Policy, applicable transfer requirements, processor contracts, and jurisdiction-specific law.

The cookie banner should not be used as a substitute for required cross-border transparency or contractual safeguards.

31. Security

Escortifys will apply safeguards appropriate to tracking and preference data, including access controls, secure configuration, vendor restrictions, integrity protections, and periodic scans or audits of deployed technologies.

Cookie values should not contain passwords, raw government identifiers, raw verification documents, private safety-report text, or other sensitive content.

32. Jurisdiction-specific rules

Cookie, device-storage, tracking, advertising, and consent laws vary. Escortifys may show different banners, default settings, cookie categories, consent models, opt-out controls, or technologies by jurisdiction.

Where a jurisdiction imposes stricter rules for sensitive personal information, targeted advertising, sale or sharing, tracking pixels, device fingerprinting, or consent, Escortifys will apply the stricter local requirement.

33. Cookie settings and browser controls

Users may be able to manage non-essential technologies through Escortifys Cookie Settings, browser settings, device settings, privacy extensions, opt-out preference signals, or third-party controls.

Blocking all cookies at the browser level may prevent login, session security, saved preferences, or other functions that genuinely rely on strictly necessary storage.

34. Changes and contact

Escortifys may update this Policy when technologies, vendors, purposes, consent requirements, or laws change. Material changes to non-essential tracking may require renewed notice or consent.

Platform: Escortifys.

Privacy / cookie inquiries: [TO BE INSERTED]

Cookie Settings: [TO BE INSERTED AT LAUNCH]

Legal notices: [TO BE INSERTED]

Operator, controller, 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 - Live cookie inventory requirements

Do not publish a guessed inventory

Before public launch, perform a technical scan of production and populate the live inventory. Re-scan after material code, tag-manager, vendor, payment, verification, analytics, advertising, or embedded-content changes.

Inventory field	Required entry
Name / key	Exact cookie or storage key
Provider / domain	Escortifys or third-party domain setting/accessing it
Technology	Cookie, local storage, pixel, SDK, fingerprint, server-side tag, etc.
Category	Necessary, preference, analytics, advertising, security, age/verification, other
Purpose	Plain-language specific purpose
Data / identifiers	What the technology stores or transmits
Duration	Session or stated expiry/retention
Third-party use	Whether vendor uses data only for Escortifys or for its own purposes
Consent status	Required before use, exempt/necessary, opt-out, or jurisdiction-dependent
Sensitive-page restriction	Pages/events where the technology must be blocked

Appendix B - Consent-banner standard

- First layer: brief explanation of purposes plus Accept All, Reject Non-Essential, and Manage Settings where the applicable regime uses consent.
- No optional tracker fires before required consent.
- Accept and reject choices should have comparable prominence where necessary for freely given consent.
- Second layer: categories off by default unless strictly necessary or another lawful model applies.
- Separate analytics, advertising/targeting, preference/functionality, and other optional purposes where granularity is appropriate.
- Do not bundle consent for cookies with Terms acceptance, age verification, subscription purchase, or Provider verification.
- Provide a persistent Cookie Settings link or equivalent method to withdraw/change consent.
- Record consent version/time without turning the consent log into an analytics identifier.
- Respect qualifying browser/device privacy signals where required.
- Re-consent when purposes or vendors change materially enough that prior consent no longer covers the processing.

Appendix C - Internal legal and implementation notes

INTERNAL - REMOVE BEFORE PUBLIC POSTING

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

C1. Project-record basis

- The Escortifys project record states that analytics must avoid leaking personal/sensitive data and that only approved aggregate metrics should be tracked after privacy review.
- The project record states that analytics/tracking was still a discussion/approval item and that no real analytics tracking had been implemented at the documented handoff stage.
- Anti-bot planning contemplated CAPTCHA/Turnstile, email and phone verification, rate limits, duplicate checks, suspicious URL/domain checks, reputation/risk signals, and moderation queues, but exact anti-bot implementation should not be exposed publicly.
- Current public reviews, provider-safety reports, payments, messaging, booking/contact exchange, and verification workflows were not confirmed live at the cited development stage; therefore this Policy does not invent trackers associated with those features.

C2. Canada

Canada does not have one single cookie statute equivalent to the EU ePrivacy Directive. PIPEDA and substantially similar provincial privacy laws can apply where cookies, identifiers, pixels, or other technologies collect, use, or disclose personal information. The Office of the Privacy Commissioner has long treated online behavioural advertising and third-party tracking as potentially involving personal information and emphasizes meaningful transparency and effective choice.

CRTC guidance under Canada's Anti-Spam Legislation states that cookies, HTML, and JavaScript can fall within deemed-consent rules for installation of computer programs where the person's conduct makes consent reasonable. That CASL rule does not eliminate separate PIPEDA/privacy obligations concerning the personal information collected through those technologies.

Implementation consequence: do not treat 'CASL deems cookie consent' as a blanket permission for sensitive tracking or behavioural advertising. On Escortifys, the sensitivity of adult-use context supports a conservative opt-in model for optional third-party tracking even where a narrower Canadian legal analysis might permit opt-out in a particular circumstance.

C3. European Union / EEA

Article 5(3) of the ePrivacy Directive, as implemented by Member States, requires clear information and consent for storing information on or accessing information from terminal equipment, subject to limited exceptions including storage/access strictly necessary to provide a service explicitly requested by the user.

The EDPB Cookie Banner Taskforce report records enforcement consensus that pre-ticked boxes and merely continuing to browse do not create valid consent, and that withdrawal should be as easy as giving consent. European supervisory authorities have also treated misleading visual design and making 'accept' materially more prominent than 'reject' as capable of undermining freely given consent.

Implementation consequence: for EEA visitors, block non-essential cookies/pixels/storage before consent; provide a genuine reject path; maintain a settings/withdrawal control; and use a Member-State review for local variations.

C4. United Kingdom

The ICO published final Storage and Access Technologies guidance on 29 April 2026. It addresses cookies, tracking pixels, device fingerprinting, and similar technologies under PECR and, where relevant, UK GDPR. The core rule remains that users must be told what non-exempt storage/access technologies do and consent must be obtained before non-essential use; exemptions apply to genuinely necessary technologies and certain other cases introduced by UK law.

Implementation consequence: build the UK banner and inventory around the 2026 ICO Storage and Access Technologies guidance rather than older cookie-only wording. Re-check regulation 6/online-advertising developments before launch because ICO regulatory work in this area is continuing.

C5. California / United States

California's CCPA statute and regulations, effective in their current 2026 form, require covered businesses that sell or share personal information to process qualifying opt-out preference signals. CalPrivacy identifies Global Privacy Control as an example of a signal consumers can use to opt out of sale/sharing. California's definition of 'sharing' can reach cross-context behavioural advertising even where no money changes hands.

Implementation consequence: if Escortifys becomes subject to the CCPA and engages in sale/sharing as defined there, honour qualifying signals such as GPC and ensure cookie/tag-manager settings actually stop the covered activity. Other U.S. states require a separate targeted-advertising/sale/profiling matrix.

C6. Australia

The OAIC's tracking-pixel guidance states that the Privacy Act does not prohibit tracking pixels but organizations must conduct due diligence, minimize personal information, understand third-party use and overseas disclosures, and generally prevent sensitive information from being disclosed through third-party pixels. The OAIC says express opt-in consent should generally be sought if sensitive information is likely to be collected and disclosed through a tracking pixel.

Implementation consequence: given Escortifys' subject matter, avoid third-party pixels on pages where sensitive information could be revealed simply by page context. A generic cookie notice is not enough if a pixel is silently transmitting sensitive information.

C7. Recommended Escortifys tracking posture

- Launch with the smallest possible tracker set: strictly necessary security/session/consent technologies first.
- Do not deploy third-party advertising pixels at initial launch unless separately approved after privacy/legal review.
- Prefer first-party, aggregate, privacy-preserving analytics and avoid cross-site identifiers.
- Block analytics and advertising entirely on ID verification, age assurance, private safety/fraud, legal-reporting, private-message, and other highly sensitive routes unless a documented exception is approved.
- Do not place sensitive search terms, profile attributes, user IDs, phone/email, precise location, or report categories into analytics URLs or event parameters.
- Implement a consent-management platform or equivalent control only after verifying that it actually prevents non-essential tags before consent and actually stops them after withdrawal.
- Treat tag-manager configuration as code: review, version, test, and audit it.
- Run automated cookie/tag scans and manual network inspections before launch and after material releases.
- Do not use session replay on sensitive areas unless a specific privacy impact assessment establishes necessity and safe redaction; default is no session replay.
- Do not use fingerprinting to resurrect advertising identity after rejection/withdrawal.
- Respect GPC/qualifying opt-out signals where legally required and consider respecting them more broadly as a privacy-enhancing default.

C8. Production facts still required

- Actual analytics product(s), if any.
- Actual advertising/affiliate pixels or conversion APIs, if any.
- Consent-management platform, if any.
- Tag manager, if any.
- Hosting/CDN security cookies and bot-protection provider.
- Authentication/session cookie names and durations.
- Payment-provider cookies once payments are live.
- Verification/age-assurance vendor storage technologies once selected.
- Embedded media/social/map vendors, if any.

- Exact cookie/local-storage inventory and domains.
- Consent categories and regional banner logic.
- GPC/opt-out-preference-signal implementation.
- Retention/expiry settings for analytics identifiers.
- Whether any session replay or heat-mapping is contemplated.

C9. Official/current sources reviewed

- Office of the Privacy Commissioner of Canada, guidance and findings on online behavioural advertising, cookies, tracking and meaningful consent.
- Canadian Radio-television and Telecommunications Commission, CASL guidance and FAQs concerning cookies, HTML, JavaScript, and deemed consent for computer-program installation.
- European Union, Directive 2002/58/EC (ePrivacy Directive), Article 5(3), and EDPB Cookie Banner Taskforce report.
- United Kingdom Information Commissioner's Office, final Storage and Access Technologies guidance published 29 April 2026 and current cookies/similar-technologies materials.
- California Privacy Protection Agency / CalPrivacy, CCPA statute and regulations effective 1 January 2026, including opt-out preference signal rules and Global Privacy Control guidance.
- Office of the Australian Information Commissioner, Tracking pixels and privacy obligations guidance.

Publication status

Document 8 is substantively complete as a global policy framework. It is not publication-ready until a production cookie/tag scan confirms the actual technologies, vendors, purposes, data fields, domains, retention periods, and consent requirements. Populate or link the live inventory, test the consent manager and privacy signals, insert contact/settings links, then remove Appendix C.