

ESCORTIFYS

GLOBAL PRIVACY POLICY

Document 2

PRE-PUBLICATION FINAL DRAFT

Document status

This document is drafted as the global master privacy policy for Escortifys. It must be conformed to the final production data map, vendor list, retention settings, legally required controller/operator disclosures, and privacy contact before public launch.

Draft date: 21 August 2026

Canadian base • Global service architecture • Regional mandatory rights preserved

1. Who We Are and What This Policy Covers

Escortifys is a global online platform. In this Privacy Policy, “Escortifys,” “we,” “us,” and “our” refer to the operator of the Escortifys service.

This Policy explains how we collect, use, disclose, retain, protect and otherwise process personal information when you visit Escortifys, create or use an account, publish or interact with listings, purchase platform products, communicate with us, submit reports or disputes, use verification features, or otherwise interact with the service.

This Policy is global. Privacy rights and legal obligations differ by jurisdiction. Where mandatory local law gives you stronger or additional rights, those rights apply. Regional notices or addenda may supplement this Policy without replacing its global baseline.

No promise of literal anonymity

Escortifys is designed for discretion and data minimization, but we do not promise that use of the service is anonymous. Account, device, security, verification, transaction, public-listing and legal-process records may identify or be linkable to an individual.

2. Privacy Principles

- Collect only information reasonably necessary for defined platform, safety, security, verification, legal and business purposes.
- Use sensitive information only for purposes that justify its collection, with heightened safeguards and consent where required.
- Separate public listing information from restricted account, verification, moderation and safety information.
- Do not sell personal information for monetary consideration.
- Do not use government identity documents, biometric verification data, restricted safety records, private support/legal communications or precise geolocation for behavioural advertising.
- Do not make a single restricted safety report, standing alone, an automatic final determination about a person.
- Provide access, correction, deletion, portability, objection or other rights where required by applicable law.
- Require lawful authority before disclosing non-public information to government or law-enforcement bodies, except where disclosure is otherwise required or lawfully permitted.
- Retain information only for as long as reasonably necessary, subject to safety, fraud, legal, accounting and record-preservation requirements.

3. Adult-Only Service

Escortifys is not directed to children or minors. You must be at least 18 years old and must also satisfy any higher age requirement imposed by applicable law or by the rules for a particular feature or jurisdiction.

We may collect age-attestation, age-assurance or identity-verification information to enforce this rule. If we reasonably believe that an account belongs to a minor, we may restrict or terminate the account, remove associated content, investigate the circumstances, make legally required reports, and retain limited information where lawful and reasonably necessary to prevent re-registration, protect safety or comply with legal obligations.

We do not use parental consent as a mechanism to permit minors to use Escortifys.

4. Personal Information We May Collect

The information we collect depends on how you use the service and which features are active in your jurisdiction. The categories below describe the data architecture Escortifys is designed to use.

Category	Examples
Account and contact information	Name or pseudonym, username, email address, phone number where used, date of birth or age status, account credentials, language, country/region and account preferences.
Public profile and listing information	Display name, profile text, approximate service area or location, photographs or other approved media, rates or price information where permitted, contact details you choose to publish, availability

	or listing attributes, verification badges and other information you deliberately make public.
Sensitive profile information	Information you choose to provide that may reveal sex life, sexual orientation, gender identity, health-related information or other legally protected sensitive characteristics. We limit collection and use of such data to the purposes disclosed at collection and as permitted by law.
Verification information	Age/identity verification results; government-issued identification, selfie/liveness material or biometric-derived verification data only where a verification method requires it and after appropriate notice; verification timestamps, status, provider and audit records.
Device, log and security information	IP address, browser/device type, operating system, timestamps, session identifiers, cookie identifiers, approximate location derived from IP, login events, security events, rate-limit events and other fraud/abuse signals.
Location information	Approximate location may be inferred from IP or chosen by you for discovery. Precise device geolocation is collected only where the feature exists, you activate it, and applicable law permits the processing.
Uploads and media metadata	Images, approved media and associated technical metadata. Escortifys is designed to strip unnecessary embedded metadata from public uploads where technically feasible, while retaining security or evidentiary information only where justified.
Communications and support	Messages to support, legal/privacy requests, moderation correspondence, reports, appeals, takedown requests, verification disputes and attachments you submit.
Reviews and reputation information	Ratings, review text, provider responses, moderation decisions, dispute records and evidence submitted in connection with reviews, if those features are activated.
Restricted safety, fraud and abuse information	Reports, incident dates, structured safety categories, evidence references, moderation notes, enforcement history, anti-fraud signals and audit logs. Certain safety records may be access-restricted and are not public.
Platform purchase information	Billing name/address, transaction identifiers, subscription or promotional product purchased, price, currency, tax information, payment status and limited payment metadata received from processors. Escortifys does not process payment for offline user-advertised services.
Information from others	Reports, complaints, verification information or evidence submitted by another person that concerns you. We assess such information for relevance, accuracy, necessity and fairness before relying on it.
Derived or inferred information	Fraud-risk, spam-risk, duplicate-content, account-reputation or moderation signals generated from permitted data. We do not treat a risk score as infallible proof of misconduct.

5. Information That Is Public

Information you deliberately publish in a public profile or listing is public. Public information may be viewed, copied, indexed, cached, archived, photographed, screenshotted or redistributed by third parties. Escortifys may use technical and contractual controls against unauthorized scraping or misuse, but we cannot guarantee that third parties will not copy information that you choose to publish.

Before publishing, consider whether you want a phone number, precise address, legal name or other identifying detail to be visible. Escortifys should not require public disclosure of information that is unnecessary for the listing.

Removing content from Escortifys does not necessarily remove copies independently retained by search engines, archives, recipients or third parties, although we may take reasonable steps to support de-indexing or removal rights where applicable.

6. Sensitive and Special-Category Information

Escortifys may process information that is highly sensitive because of the nature of the service. Depending on jurisdiction, this can include information about sex life, sexual orientation, gender identity, precise location, government identifiers, identity documents, biometric verification, private communications, safety allegations and other information capable of causing significant harm if misused.

We apply heightened controls to such information. Where applicable law requires express or explicit consent, a separate condition for processing, a privacy impact assessment, or enhanced notice, Escortifys will implement that requirement before activating the relevant processing.

- Sensitive information will not be collected merely because it might be useful later.
- Sensitive information will not be used for behavioural advertising.
- Raw identity documents and biometric verification data will not be displayed publicly.
- Restricted safety records will not be exposed through public profiles or ordinary member search.
- Access will be limited according to role, purpose and need to know.
- Where a feature can operate with a verification result rather than a copy of the underlying document, the verification result should be retained instead of the raw document.

7. How We Use Personal Information

We may use personal information for the following purposes, subject to applicable law and the availability of the relevant feature:

- Create, authenticate and maintain accounts.
- Display and manage listings and profile information that users choose to publish.
- Provide search, discovery, location and visibility functions.
- Verify age, identity, account ownership, provider status or media authenticity where those controls are offered.
- Process payments for Escortifys platform products such as subscriptions, featured placement, verification or promotional visibility. Escortifys does not collect or transmit payment for offline user-advertised services.
- Moderate listings, images, reviews, links, messages or other content and enforce the Terms and platform policies.
- Detect and investigate bots, spam, impersonation, scams, account compromise, duplicate content, prohibited conduct, trafficking indicators, exploitation, threats and other safety or security risks.
- Operate restricted safety, fraud and abuse systems if and only if those systems receive the required legal, privacy and product approval.
- Handle user reports, disputes, takedown requests, correction requests, appeals and safety escalations.
- Communicate administrative, security, legal and service notices.
- Measure performance and understand aggregate service use using privacy-reviewed analytics.
- Maintain audit logs, evidence trails, records of consent and policy acceptance, and records necessary to demonstrate compliance.
- Comply with lawful obligations, preserve evidence, establish or defend legal claims and respond to valid legal process.
- Prevent re-registration or repeated abuse after serious policy violations where lawful and proportionate.
- Conduct internal product, privacy, safety and security testing using minimized, de-identified, synthetic or otherwise appropriately protected data where feasible.

8. Consent, Legal Authority and Regional Legal Bases

Canadian privacy law generally focuses on appropriate purposes, accountability, meaningful consent, limiting collection, safeguards, access and related fair-information principles rather than using the GDPR's terminology for every processing activity. Escortifys will seek meaningful consent where required and will seek express consent where the sensitivity, reasonable expectations or risk of harm makes that appropriate.

For individuals in the European Economic Area or United Kingdom, where the GDPR or UK GDPR applies, we will identify an applicable Article 6 lawful basis and, for special-category data, an applicable Article 9 condition before processing. Depending on the activity, the basis may include performance of a contract, compliance with legal obligations, legitimate

interests that are not overridden by individual rights, protection of vital interests, or consent. Special-category processing may require explicit consent or another legally available condition.

Other jurisdictions may use different legal concepts, including notice-and-choice, opt-out rights, reasonable-purpose tests or specific statutory permissions. Nothing in this Policy is intended to reduce mandatory rights.

Where consent is the basis for processing, you may withdraw it prospectively, subject to legal or contractual restrictions and to consequences that are explained at the time of withdrawal. Withdrawal does not invalidate processing already lawfully performed.

9. Identity, Age and Media Verification

Verification is intended to establish limited facts - for example, age, identity, control of an account, or correspondence between a person and submitted media. Verification is not a guarantee of character, legality, safety, health status, authenticity of every statement, or future conduct.

If a verification process requires government identification, selfie/liveness checks or biometric matching, Escortifys will provide a feature-specific notice explaining the information collected, purpose, provider, retention approach and choices before collection. Where practicable, Escortifys will retain the verification outcome and audit record rather than the raw identity document.

We will not adopt a government identifier as Escortifys' ordinary account identifier where prohibited by law.

If an external verification provider independently determines purposes or retains information under its own legal obligations, its privacy notice may also apply. We will identify material verification providers before a production verification feature is activated.

10. Automated Tools, Moderation and Profiling

Escortifys may use automated or semi-automated tools to assist with spam detection, duplicate-content detection, suspicious-link analysis, device/IP risk analysis, account security, content moderation, age/identity checks, ranking or other platform-protection functions.

Automated indicators are signals, not unquestionable findings. Where a decision has a legal or similarly significant effect and applicable law gives a right to human intervention or review, Escortifys will provide an appropriate review mechanism.

A single restricted safety report will not, by itself, automatically produce a permanent ban. Serious emergency content may be temporarily restricted pending review where necessary to protect people or the service.

If Escortifys introduces materially new profiling or solely automated decision-making, the privacy notice and consent/rights mechanisms will be updated before activation where required.

11. Restricted Safety, Fraud and Abuse Records

Escortifys may maintain restricted records to protect users, providers, staff and the service from safety threats, fraud, harassment, impersonation, exploitation, repeated abuse and serious policy violations. Some records may originate from reports submitted by authorized users or third parties.

These records are not ordinary public reviews. They are subject to restricted access, purpose limitation, moderation, accuracy controls, audit logging, retention limits and correction/dispute procedures where applicable.

- We seek to collect only information relevant to the safety or abuse purpose.
- We do not permit discriminatory reporting based on protected characteristics.
- We do not permit doxxing, revenge reporting, extortion or knowingly false reports.
- We may ask for incident dates, supporting evidence or clarification before relying on a report.
- We may restrict access to reporter identity when disclosure would create safety, retaliation or legal concerns, subject to mandatory rights of access and procedural fairness under applicable law.
- We may preserve or disclose restricted records where required by valid legal process or where another lawful exception applies.

High-risk feature gate

Any provider-only safety-reporting system must remain inactive until its privacy, defamation, discrimination, retention, accuracy, dispute, access-control and legal-escalation rules have been approved and implemented.

12. Cookies, Similar Technologies and Analytics

Escortifys may use cookies, local storage and similar technologies for authentication, security, preferences, fraud prevention, performance and analytics. A separate Cookie Policy will describe the categories and current vendors in greater detail.

- Strictly necessary technologies may operate without optional consent where legally permitted.
- Analytics, advertising or other non-essential technologies will be subject to consent, opt-out or preference controls where required.
- Precise geolocation, profiling or similar higher-risk functions will not be activated by default where applicable law requires affirmative activation.
- We will not intentionally place sensitive profile fields, private safety-report contents or identity-document data into advertising analytics.
- Where required, we will recognize legally valid browser or device preference signals, including opt-out preference signals applicable to sale/sharing or targeted advertising.

The production Cookie Policy and consent manager must match the actual cookies, tags, SDKs and vendors in use. A copied list of fashionable tracking tools would be worse than useless.

13. When We Disclose Personal Information

We may disclose personal information only for identified, lawful and proportionate purposes, including the following:

- Public users: information you intentionally publish in a public listing or profile.
- Service providers: hosting, content delivery, security, communications, identity/age verification, payment processing for platform purchases, moderation, customer support, analytics and other processors necessary to operate the service.
- Professional advisers: lawyers, accountants, insurers, auditors, security specialists and other advisers subject to appropriate duties of confidentiality.
- Government, regulators, courts and law enforcement: when required by valid legal process or otherwise required or lawfully permitted, subject to the government-request safeguards in this Policy.
- Safety or emergency recipients: where applicable law permits disclosure to address a credible and serious threat, exploitation, child-safety issue, trafficking concern or other emergency.
- Corporate transaction recipients: prospective or actual purchasers, investors, financiers or successors in a merger, acquisition, financing, restructuring, insolvency or sale, subject to confidentiality and applicable law.
- At your direction: where you instruct or expressly authorize us to share information.

We do not sell personal information for monetary consideration. If a jurisdiction defines certain advertising disclosures as a 'sale' or 'sharing' even without payment, Escortifys will provide any consent, opt-out or preference mechanism required before engaging in that activity.

14. Payment Information

Payments made to Escortifys are for Escortifys platform products only, such as subscriptions, verification, featured placement, promotional visibility or other platform functionality. Escortifys does not receive, hold, route, settle, collect, disburse or share payment for offline user-advertised services.

Payment processors may collect card, bank, wallet or other payment credentials directly. Escortifys should receive only the payment and transaction information reasonably necessary to confirm payment, manage subscriptions, issue receipts, prevent fraud, handle disputes and meet legal/accounting requirements.

We do not promise to store full payment-card credentials and should not do so unless a compliant payment architecture specifically requires it.

15. International and Cross-Border Processing

Escortifys is operated from Canada and may use service providers, infrastructure or professional advisers located in Canada or other countries. Personal information processed in another country may be subject to that country's laws, including lawful access by courts, regulators or government authorities.

Where cross-border processing occurs, Escortifys will use contractual, technical, organizational and legal measures appropriate to the jurisdiction and sensitivity of the information. These may include processor agreements, confidentiality obligations, security requirements, transfer risk assessments, recognized adequacy mechanisms, Standard Contractual Clauses, the UK transfer mechanisms, or other lawful safeguards.

For Quebec information, privacy impact assessment requirements and cross-border considerations will be addressed where applicable. For Australian information, reasonable steps regarding overseas recipients will be taken where the Australian Privacy Principles apply.

A current list of material service-provider locations or countries should be maintained where required by law and made available through this Policy, a subprocessor page or a regional notice once the production vendor stack is final.

16. Government, Regulatory and Law-Enforcement Requests

Escortifys does not treat an informal request from an authority as automatic permission to surrender non-public user information.

- We may verify the identity, jurisdiction and authority of the requester.
- We may require a warrant, production order, subpoena, court order or other legally sufficient process where the law requires it.
- We may seek clarification, narrow an overbroad demand, object to a defective demand or challenge a demand where legally available and appropriate.
- We distinguish preservation of information from disclosure of information.
- We disclose only information reasonably responsive to lawful process, unless broader disclosure is otherwise required by law.
- We maintain records of material requests and disclosures where legally and operationally appropriate.
- We may notify the affected user before or after disclosure where legally permitted and where notice would not unlawfully compromise an investigation, court order or legitimate safety interest.
- Emergency and mandatory-reporting situations are handled under separate procedures and applicable law.

Nothing in this section prevents Escortifys from complying with a valid and binding legal obligation.

17. Data Retention and Deletion

We retain personal information only for as long as reasonably necessary for the purposes for which it was collected, including providing the service, safety and fraud prevention, disputes, legal compliance, accounting, security, enforcement and preservation of legal claims.

Retention depends on sensitivity, purpose, risk, user expectations, legal requirements and whether the information remains necessary. Data subject to a legal hold, active investigation, safety escalation, chargeback, dispute or legal proceeding may be retained beyond ordinary periods.

The following is the intended production baseline. It must be validated against the final system design and applicable legal requirements before launch.

Record	Intended baseline
Raw identity/age verification documents	Target: delete or cause the processor to delete as soon as the verification purpose is complete, ordinarily within 30 days after a final verification decision, unless a longer period is required for fraud, dispute, legal or regulatory reasons.
Verification outcome and audit record	For the active account and ordinarily up to 2 years after closure or last relevant enforcement event, unless a shorter or longer period is required by law or risk.
Public profile/listing content	While published or needed for the account; removed content may remain in restricted backups or moderation records for a limited period.
Routine security/access logs	Target: up to 12 months; serious security, fraud or enforcement events may be retained longer, ordinarily up to 24 months unless legal preservation applies.
Reviews, disputes and moderation records	While relevant to the published content or account, then ordinarily up to 24 months after final resolution unless ongoing safety, fraud or legal reasons justify longer retention.
Restricted safety/fraud reports	Periodic necessity review; target maximum of 24 months after the last relevant safety event or final resolution unless an active risk,

	repeated pattern, legal hold or statutory requirement justifies longer retention.
Support and privacy correspondence	Ordinarily up to 24 months after closure of the request, longer where required for complaint, legal or compliance records.
Platform billing/transaction records	For the period required by applicable tax, accounting, anti-fraud, chargeback and financial-record laws.
Consent and policy-acceptance records	For as long as reasonably necessary to demonstrate the consent or contractual/legal event and applicable limitation periods.
Backups	Rolling backup retention should be limited; target deletion from ordinary backup cycles within 90 days after primary deletion unless disaster-recovery or legal preservation requires longer.

Deletion from an active system may not immediately remove information from encrypted backup media. Backup copies should age out under the backup cycle and should not be restored into active use except for legitimate recovery, security or legal purposes.

We may retain limited identifiers after account closure where reasonably necessary and lawful to prevent fraud, impersonation, repeated serious abuse or prohibited re-registration. Such retention must be proportionate and access-restricted.

18. Security Safeguards

Escortifys will use administrative, technical and organizational safeguards appropriate to the sensitivity and volume of the information, the foreseeable harms from misuse, and the state of the service.

- Role-based and need-to-know access controls for restricted data.
- Encryption in transit and appropriate protection for sensitive stored data where technically applicable.
- Credential protection, rate limiting, monitoring and anti-abuse controls.
- Audit logs for material moderation, verification and administrative actions.
- Secure development, vulnerability remediation and change-control practices appropriate to the system.
- Vendor due diligence and contractual privacy/security obligations.
- Separation of public listing data from restricted verification, safety and legal records where feasible.
- Metadata minimization for uploaded public media where technically feasible.
- Incident response, breach assessment, containment and notification procedures.

No security system is perfect. We do not guarantee that unauthorized access, loss, misuse or disclosure can never occur.

19. Privacy and Security Incidents

If a breach of security safeguards or other privacy incident occurs, Escortifys will investigate, contain and assess the incident and will notify affected individuals, regulators or other organizations when required by applicable law.

Because information associated with an adult-oriented platform can create heightened risks of humiliation, reputational harm, discrimination, stalking, extortion or personal safety consequences, the sensitivity of the information will be treated as a central factor in incident assessment.

Escortifys will maintain breach and incident records for the period required by applicable law.

20. Your Privacy Rights

Depending on where you live and which law applies, you may have some or all of the following rights:

- Know or be informed about the personal information we collect, use and disclose.
- Access personal information we hold about you.
- Correct inaccurate or incomplete personal information.
- Request deletion or erasure, subject to lawful exceptions.
- Withdraw consent where processing depends on consent.
- Object to or restrict certain processing.
- Receive eligible information in a portable, commonly used or machine-readable format.

- Limit certain uses or disclosures of sensitive personal information.
- Opt out of sale, sharing, targeted advertising or certain profiling where applicable.
- Request human review or challenge certain solely automated decisions where applicable.
- Request de-indexing or cessation of dissemination where applicable.
- Complain to Escortifys and, where applicable, to a privacy regulator or supervisory authority.

We may need to verify your identity before fulfilling a request. We will not require more verification information than is reasonably necessary for the request. We may deny or limit a request where permitted by law, including where disclosure would improperly reveal another person's information, compromise security, prejudice an investigation, or conflict with a legal preservation obligation. Where required, we will explain the reason.

21. Regional Privacy Rights

21.1 Canada

For Canadian commercial activities, federal PIPEDA may apply, including to interprovincial and international personal-information flows. Depending on the circumstances, provincial private-sector privacy laws may also apply, including in Quebec, Alberta and British Columbia. Escortifys will maintain a privacy-accountability function, identify purposes, seek meaningful consent where required, limit collection/use/disclosure/retention, apply safeguards, provide access and correction rights, and maintain complaint procedures.

Quebec residents may have additional rights and protections, including requirements concerning privacy impact assessments, default privacy settings, profiling/location technologies, confidentiality incidents, de-indexing, portability and automated decisions. Where Quebec law applies, those requirements will be implemented for the relevant processing.

21.2 European Economic Area

Where the EU GDPR applies, individuals may have rights of access, rectification, erasure, restriction, portability, objection and rights concerning solely automated decision-making, along with the right to complain to a supervisory authority. Special-category data, including data concerning sex life or sexual orientation and certain biometric data, receives enhanced protection.

Where required because Escortifys offers services to individuals in the EEA without an establishment there, Escortifys will appoint and identify an EU representative before the relevant processing begins. International transfers will use a lawful transfer mechanism where required.

21.3 United Kingdom

Where UK data-protection law applies, individuals may have rights to be informed, access, rectification, erasure, restriction, portability, objection and protections concerning automated decision-making and profiling. Special-category information includes data concerning sex life, sexual orientation and biometric identification data. UK representative and international-transfer requirements will be addressed where applicable.

21.4 California and Other U.S. States

Where a U.S. state privacy law applies, residents may have rights to know/access, delete, correct, opt out of sale or sharing, opt out of targeted advertising or certain profiling, obtain portability, limit certain uses of sensitive personal information, and appeal certain request decisions. California treats information such as precise geolocation, government identifiers, certain private communications, biometric identification data, and information about sex life or sexual orientation as sensitive personal information.

Escortifys does not sell personal information for monetary consideration. Where a state treats advertising-related disclosures as 'sharing' or otherwise grants opt-out rights, the required mechanism will be provided before the relevant activity is used.

21.5 Australia and Other Jurisdictions

Where the Australian Privacy Act and Australian Privacy Principles apply, sensitive information receives heightened protection and cross-border disclosures may carry specific accountability obligations. Similar local rights and transfer rules may apply in New Zealand and other jurisdictions.

This global Policy does not attempt to reproduce every national privacy statute. Mandatory local rights apply notwithstanding any narrower wording in this Policy, and regional notices may be added before Escortifys actively targets a jurisdiction.

22. Account Closure, Suspension and Data Access

Closing, suspending or terminating an account does not automatically erase every record. We may retain information necessary for billing, fraud prevention, abuse prevention, legal obligations, disputes, safety, enforcement history and legal claims.

Where reasonably feasible and legally permitted, suspension for non-payment of a platform subscription should not be used as a mechanism to hold a user's own eligible data hostage. Access/export rights, if legally required, remain subject to identity verification and safety/legal restrictions.

Public listing information will be removed or de-indexed according to the account/content status and applicable law, but third-party copies may persist outside Escortifys.

23. Marketing Communications

Administrative, security, legal and transactional messages may be necessary to operate an account and may not be optional. Marketing communications will be sent only where permitted by applicable law, including Canada's anti-spam rules where applicable.

You may unsubscribe from non-essential marketing using the mechanism provided in the message or account settings. Unsubscribing from marketing does not prevent necessary service or legal notices.

24. Third-Party Links and External Services

Escortifys may contain links to third-party websites or services. We do not control their privacy practices. Information you provide directly to a third party is governed by that third party's policies, subject to applicable law.

External links do not authorize a third party to receive restricted Escortifys data. Any technical data-sharing integration must be separately assessed and disclosed.

25. Business Transfers and Ownership Changes

If Escortifys or relevant assets are involved in a financing, reorganization, merger, acquisition, insolvency, sale or transfer, personal information may be disclosed or transferred as part of that transaction where permitted by law. We will seek appropriate confidentiality and use restrictions and provide notice where required.

A successor may use personal information only as permitted by applicable law and the privacy commitments that bind the transferred information, unless a lawful new notice or consent process applies.

26. Changes to This Policy

We may update this Policy to reflect changes in law, technology, vendors, security practices, product features or data processing. The current version will identify its effective or revision date.

Where a change is material, particularly where it introduces a new use of sensitive personal information, a new category of recipient, or a materially different purpose, we will provide additional notice and obtain consent where required before the new processing begins.

27. Privacy Contact and Complaints

Escortifys is responsible for privacy governance of the service. Before public launch, the following information must be finalized or made available in the manner required by applicable law:

- Privacy Officer / responsible title: [TO BE CONFIRMED]
- Privacy email: [TO BE CONFIRMED]
- Legal/service address: available upon a valid request where appropriate, and otherwise disclosed where applicable law requires proactive disclosure.
- General support contact: [TO BE CONFIRMED]

Privacy requests and complaints should be directed to the Privacy Officer. We will investigate complaints and respond within the period required by applicable law. You may also have the right to complain to the Office of the Privacy Commissioner of Canada, a provincial privacy regulator, an EU/EEA supervisory authority, the UK Information Commissioner's Office, the California Privacy Protection Agency, the Office of the Australian Information Commissioner, or another competent authority, depending on where you live and which law applies.

28. Relationship to Other Escortifys Policies

This Privacy Policy should be read together with the Escortifys Global Terms of Service, Cookie Policy, Acceptable Use and Content Policy, Advertising and Listings Policy, Safety and Reporting Policy, and any applicable regional privacy notice. If a regional mandatory privacy rule conflicts with this Policy, the mandatory rule governs to the extent of the conflict.

PRE-PUBLICATION IMPLEMENTATION APPENDIX

Remove or separate before live publication

The material below is an implementation and legal-review checklist. It should not appear as part of the public-facing privacy notice once the production data architecture is finalized.

A. Production facts that must be confirmed

- Whether any launch jurisdiction requires proactive disclosure of the controller/operator identity, legal form, service address or similar particulars; if so, implement only the required disclosure in the legally appropriate context.
- Serviceable business/legal address and Privacy Officer contact.
- Production hosting/CDN countries and all material subprocessors.
- Identity/age verification vendor, whether raw ID or biometric data is processed, and retention/deletion controls.
- Payment processor(s) for Escortifys platform products and the exact payment metadata returned to Escortifys.
- Authentication, email/SMS, support, analytics, moderation, anti-bot and security vendors.
- Exact cookies, local-storage keys, SDKs, pixels and tags in production.
- Whether precise geolocation exists and whether it is opt-in.
- Whether user-to-user messaging exists; if so, message storage, moderation scope, encryption model and retention.
- Whether reviews are live and the exact moderation/dispute/retention workflow.
- Whether restricted safety reports are live; if so, complete privacy impact assessment, lawful-purpose analysis, access model, accuracy/dispute process and retention controls first.
- Final retention settings in databases, logs, object storage, backups, processor systems and audit logs.
- Data export/deletion workflow and identity-verification method for privacy requests.
- Regional consent manager and Global Privacy Control / opt-out signal handling where required.

B. High-risk processing requiring privacy impact review before activation

- Government-ID collection or storage.
- Face matching, liveness, biometric templates or biometric identification.
- Precise location tracking.
- Restricted provider safety reports or client safety notes.
- Solely automated bans or material account decisions.
- Profiling that uses sensitive profile attributes.
- Cross-context behavioural advertising or data sharing with ad-tech partners.
- Large-scale monitoring of private messages or communications.
- Cross-border transfer of highly sensitive information.
- New use of user data for general-purpose AI/model training.

C. Research basis used for this draft

Source	Relevance	Reference
Canada - Office of the Privacy Commissioner	PIPEDA Fair Information Principles; meaningful consent; accountability; openness; cross-border processing; breach guidance.	https://www.priv.gc.ca/
Quebec - Commission d'accès à l'information	Law 25 changes concerning privacy impact assessments, default privacy settings, profiling/location technologies, confidentiality incidents, portability and automated decisions.	https://www.cai.gouv.qc.ca/
European Union - GDPR	Regulation (EU) 2016/679, including special-category data, transparency, individual rights, security, transfers and impact assessments.	https://eur-lex.europa.eu/eli/reg/2016/679/oj
United Kingdom - ICO	UK GDPR guidance on special-category data, individual rights, privacy information and automated decision-making/profiling.	https://ico.org.uk/
California - CCPA	CCPA/CPRA rights and treatment of sensitive	https://cppa.ca.gov/

	personal information.	
Australia - OAIC	Australian Privacy Principles, sensitive information and cross-border disclosure obligations.	https://www.oaic.gov.au/
Comparator - Locanto	Current privacy-policy architecture for a global classifieds service, used only as a structural comparator, not copied as legal authority.	https://www.locanto.com/g/info/privacy/

Publication gate

Do not publish this Privacy Policy as 'final' until the production data-flow map, vendor/subprocessor list, retention schedule, verification system, cookie inventory, regional targeting and privacy contact details have been reconciled against the text. A privacy policy that promises controls the product does not actually have is a liability document wearing a tie.