

Lythe Privacy Policy

Last updated: 21 October 2026

1. Introduction

This Privacy Policy explains how Lythe Inc. and its applicable affiliates, including Lythe Pte. Ltd. (collectively and as applicable, “Lythe,” “we,” “us,” or “our”), collect, use, disclose, store, and protect personal data in connection with Lythe’s products, websites, applications, public demos, simulation tools, integrations, documentation, and related services, including Fraser Simulation Studio (collectively, the “Services”).

Fraser Simulation Studio is Lythe’s managed AI-powered simulation and automated evaluation service for testing websites, product flows, visual experiences and Android applications using AI personas and subagents. Customers request simulations and provide their needs and permitted inputs through the vendor or client portal or another enabled interface. Lythe manually verifies testing authority, operates and monitors accepted simulations within agreed guardrails and delivers agreed reports. Required Customer confirmations remain conditions of execution. At launch, Lythe Inc. provides the Services to business customers in the United States. Lythe Pte. Ltd. is the contracting provider only where expressly identified in a separately executed customer agreement. Public access to informational websites does not establish eligibility for the Services or restrict rights under applicable privacy law.

The Services may be used to create, configure, test, evaluate, and improve AI personas, subagents, simulations, automated evaluation workflows, and related outputs. Simulation tools may generate AI persona feedback, product critiques, evaluation reports, simulated user reactions, messaging analysis, and product research outputs. This Privacy Policy is intended to help users, customers, End Users, research subjects, and business partners understand how personal data may be handled in connection with the Services.

2. Scope of This Policy

This Policy applies to personal data we process in connection with the Services, including information collected through our websites, product dashboards, public demos, customer support, sales interactions, events, simulation workflows, and product evaluation tools.

Lythe Inc. is responsible for personal data Processing for purposes it independently determines in operating its websites and Services. Where Lythe Processes Customer Personal Data on a customer’s behalf, the DPA governs that Processing. Any different contracting provider and its responsibilities must be expressly identified in the executed customer agreement.

When we process personal data on behalf of a business customer under a written agreement, the applicable Lythe entity may act as a service provider, data processor, or data intermediary, depending on the applicable law and the relevant processing activity. In those cases, the

customer is generally responsible for providing required notices, obtaining required consents, establishing lawful bases, and instructing Lythe on how to process personal data, subject to Lythe's own obligations under applicable law. Our Data Processing Addendum or customer agreement may further govern that processing.

This Policy does not apply to third-party websites, applications, products, or services that are not controlled by Lythe, even if they link to or integrate with the Services. Submitting a third-party website, URL, screenshot, prototype, or product flow for analysis through Fraser Simulation Studio does not make Lythe responsible for that third-party service.

3. Information We Collect

3.1 Account and Business Contact Information

Name, company name, role, email address, phone number, billing contact, and account credentials.

Information provided during onboarding, sales calls, demos, pilot programs, customer support, enterprise procurement, and product waitlists.

Communications with us, including messages, support tickets, feedback, surveys, demo requests, application forms, and meeting notes.

3.2 Customer Content, Agent Configuration, and Simulation Configuration

Prompts, scripts, instructions, knowledge base content, agent names, AI persona configurations, simulation settings, evaluation criteria, workflows, tools, API configurations, and business rules submitted to the Services.

Testing and persona-enrichment content must remain within Permitted Inputs under the Terms of Service: synthetic or truly anonymized information; ordinary, non-sensitive personal details incidental and necessary to evaluate authorized public pages; and real customer records, feedback or conversation materials separately approved through a Data Approval completed before receipt or access. Lythe recommends synthetic sample records for authenticated testing. Safeguarded test accounts remain required; real customer records must remain hidden unless Lythe expressly approves the particular records, target access and safeguards in a Data Approval before receiving or accessing them. Sensitive or regulated data, children's data, identifiable raw replay and re-identification keys remain prohibited. Replacing names or leaving data unlabeled does not by itself make information anonymous.

Customer content may include permitted files, datasets, screenshots, public pages, URLs, prototypes, product flows, APKs, research notes and feedback. Incidental public-page personal details, such as staff names, professional photographs, bylines and job titles, are processed only as necessary for the approved page or product evaluation, without profiling individuals. Real

customer records, feedback or conversation materials may include necessary ordinary, non-sensitive personal information only within a Data Approval completed before receipt or access. Customer-selected integrations remain subject to the same limits and do not authorize receipt of identifiable CRM records or private live-user information without a specific prior Data Approval covering the connection, records and use. Account, billing, contact and service-usage information is handled separately as described in this Policy.

3.3 Conversation Information and Approved Feedback Used for Persona Enrichment

Customers may supply synthetic or truly anonymized summaries, notes, transcripts or interaction information. Real customer records, feedback, conversation-derived material or transcripts containing necessary ordinary, non-sensitive personal information may be received only after a separate written Data Approval defines the source and any target access or connection involved, necessary information, Customer-specific purpose, lawful authority, required notices and consents, minimization, secure transfer, approved providers, access and retention. Recordings require an enabled feature and specific approval. Initial approval review uses a description or a sample already within the permitted boundaries; unapproved personal source material must not be sent for review. Sensitive information and other prohibited categories must be removed before transfer.

Conversation analysis outputs, including topics, intents, sentiment or tone indicators, recurring pain points, feature requests, objections, product feedback, and persona-enrichment signals.

Within the available feature scope and any required Data Approval, Lythe may label permitted feedback and conversation information and use it through prompts, retrieval or configuration to enrich synthetic personas for that Customer's own simulations. This is not identification or profiling of real individuals, training of shared or general-purpose models, or use of identifiable material for other customers. At launch, simulations must not contact real people or perform real transactions. Authenticated testing uses client-provided test environments or safeguarded test accounts. Lythe recommends synthetic sample records for authenticated testing. Safeguarded test accounts remain required; real customer records must remain hidden unless Lythe expressly approves the particular records, target access and safeguards in a Data Approval before receiving or accessing them. Outbound calling, voice-agent deployment, telemarketing, robocalling and call routing are not part of the launch offering.

3.4 Simulation, AI Persona, and Product Evaluation Data

Simulation inputs, AI persona prompts, persona profiles, product concepts, feature descriptions, user flows, messaging, positioning, onboarding flows, product screenshots, landing pages, prototypes, and related evaluation materials.

Simulation outputs, including AI persona responses, product critiques, usability observations, feature recommendations, product-market-fit hypotheses, segmentation insights, evaluation scores, reports, research-preparation outputs, and related analytics.

Research methodology information, evaluation settings, assumptions, success criteria, failure conditions, review notes, and human-feedback records associated with simulations or automated evaluations.

3.5 Usage, Device, and Technical Information

Log data, IP address, browser type, device identifiers, operating system, pages viewed, referring URLs, session activity, API requests, latency, errors, uptime information, and feature usage.

Product interaction information, including clicks, scrolling behavior, cursor or pointer movements, navigation paths, page transitions, feature interactions, timestamps, form interactions, and session replay data.

Lythe uses optional PostHog analytics and session replay on its landing website to understand usage and diagnose software and usability issues. Visitors must approve these technologies through the consent controls before they are enabled and may reject or later withdraw consent. Replay can capture page content, navigation, and interactions; masking and exclusion controls are described below. A PostHog integration inside the product is separate, optional, and contracted and controlled by the customer under the customer's own PostHog account.

Sensitive fields, including passwords, payment information, authentication credentials, API keys, security codes, and other sensitive information, are masked or excluded from session replay. Lythe does not intentionally record such information through session replay.

Security and diagnostic data used to protect the Services, detect abuse, debug issues, prevent unauthorized website testing or scraping, and maintain system reliability.

Cookies, pixels, local storage, SDKs, session replay technologies, and similar technologies used for authentication, analytics, security, preference management, and marketing where permitted.

Authorization and compliance records, including target domains and applications, Target Certifications, the customer's stated relationship to a target, references to authorization evidence, the accepting user's identity and organization, acceptance timestamps, Terms and policy versions, IP address, device or browser information, testing-scope selections, rate settings, stop events, and related audit records.

3.6 Payment and Billing Information

Business billing information includes billing contacts, invoice details, agreed service and usage terms, payment status, tax information, and transaction records needed to administer the customer's agreement. For self-serve purchases and refunds, this may include purchase,

subscription, billing-period and charge identifiers; successful-payment timestamps and time zones; the original portal-ticket submission timestamp or first refund-request email timestamp; purchase-specific report and paid-quota usage; refund requests, related communications and supporting information; request review, decline, closure and automatic-refund trigger timestamps; approval or decline decisions; and refund processing and status records.

Non-enterprise customers may make self-serve one-time purchases and purchase automatically renewing subscriptions through the account and checkout flow. Lythe uses Stripe for payment operations, including processing approved refunds to the original payment method. Recurring charge authorization arises from the subscription terms disclosed and accepted at checkout and the applicable Terms of Service, not from this Privacy Policy. Enterprise billing, payment methods and any renewal arrangements are governed by the separately executed customer agreement.

4. How We Use Information

We use personal information for the following purposes:

To provide, operate, maintain, secure, and improve the Services.

To create, configure, monitor, evaluate, and support AI personas, subagents, simulations, automated evaluators, and related workflows.

To label Permitted Inputs and analyze permitted conversation information, analytics and real feedback within a prior Data Approval to configure Customer-specific synthetic personas and support requested simulations and product evaluations.

To run simulations, generate AI persona responses, produce product critiques, evaluate user flows, analyze messaging, create reports, and support customer-requested product research workflows.

To authenticate users, manage accounts, process payments, send invoices, administer plans and usage limits, administer refund requests and related purchase-specific quota and access adjustments, and provide customer support.

To detect, prevent, investigate, and respond to fraud, spam, abuse, unauthorized website testing, security incidents, illegal activity, and violations of our terms or policies.

To analyze product usage, measure performance, debug technical issues, improve public demos, and develop new features.

To comply with legal obligations, enforce agreements, resolve disputes, and protect the rights, safety, security, and interests of Lythe, our customers, End Users, research subjects, users, business contacts, and the public.

To send administrative messages, including refund decisions and processing updates by email and in the account portal, product updates, security notices, and marketing communications where permitted by law and subject to opt-out rights.

To understand how users navigate and interact with the Services through product analytics, interaction events, and session replay.

To identify bugs, usability friction, navigation issues, failed workflows, technical errors, and product performance problems.

To verify and document assent and target authorization; prevent, investigate, and remediate unauthorized or out-of-scope testing; enforce testing boundaries; respond to Target Owners, complaints, disputes, legal process, or regulators; and protect the security, reliability, and integrity of the Services and third-party systems.

5. AI Processing, Evaluation, and Service Improvement

Lythe may process Permitted Inputs, simulation configurations, feedback and evaluation results to provide, operate, secure, support, troubleshoot and evaluate the Services under Customer instructions, applicable agreements and the DPA. This may include approved labeling, measuring performance, generating reports, investigating incidents and updating prompts, retrieval or configurations for that Customer's own use. Real customer records, feedback or conversations require Data Approval before receipt or access; this is not a service for accepting unapproved identifiable datasets for later anonymization.

Lythe does not use Customer Personal Data or identifiable inputs to train Lythe models, shared models, general-purpose models or systems for other customers. Separately approved feedback may be used through prompts, retrieval or configuration for that Customer's own synthetic personas and simulations, without training models or profiling real individuals. Lythe may also label truly anonymized information and use aggregated or de-identified information that identifies neither a customer nor an individual for analytics, security, reliability, usage measurement and product improvement, subject to applicable agreements and law.

Lythe does not permit third-party model or AI infrastructure providers to use Customer Data, call recordings, transcripts, research data, simulation inputs, AI persona outputs, or other personal data processed through the Services to train their models.

Lythe may use de-identified or aggregated information that does not identify individuals or customers to analyze service performance, security, reliability, abuse patterns, and product usage, provided that such information is handled in accordance with applicable law and applicable customer agreements.

Customers are responsible for lawful source collection, required rights, notices, consents and lawful bases, minimization and any necessary anonymization, and for supplying only Permitted

Inputs. Real customer records, feedback or conversation information requires Data Approval before receipt or access. If prohibited data, unapproved real customer records in an authenticated target, or source material outside a valid Data Approval is encountered, affected capture, testing and onward transmission must stop; Lythe must restrict access, isolate the material and notify Customer. Handling is limited to necessary containment, investigation, secure return or deletion under the DPA and law. Ordinary personal details already within approved public-page scope or a valid Data Approval are not by themselves prohibited.

6. Simulation, Bug Testing, and Synthetic Research Disclosure

Fraser Simulation Studio may enable customers to use subagents, AI personas, simulations, visual evaluations, and bug-testing workflows to analyze websites, landing pages, product flows, screenshots, prototypes, and Android application packages (APK files). These features may be used to battle-test website bugs, evaluate user flows, generate visual simulations from URLs, identify interface issues, and produce synthetic product feedback or evaluation reports.

Customers may use Fraser Simulation Studio, subagents, simulations, visual evaluations, and bug-testing workflows only on Authorized Targets as defined in the Terms of Service and must complete any required Target Certification. Customers must not use the Services to test, scrape, monitor, access, or analyze a competitor or any other third-party website, application, system, or content without the Target Owner's prior express written authorization covering the testing.

Customers are responsible for ensuring that all URLs, screenshots, APK files, product materials, customer data, and other materials submitted to the Services are lawful, authorized, and appropriate for the intended use. Customers must verify that their use of the Services does not violate any applicable laws, third-party terms of service, contractual restrictions, intellectual property rights, privacy rights, or security requirements.

Simulation outputs, AI persona responses, visual evaluations, bug-testing results, product critiques, and synthetic feedback are generated for product evaluation and research-support purposes. Customers are responsible for ensuring that these outputs are never presented as real user interactions or real customer interviews and that their synthetic origin is disclosed. Specific vulnerability, survey, or market findings may be described as independently validated only to the extent supported by appropriate independent methods, with the validation methodology and synthetic contribution disclosed. These outputs must not be presented as guaranteed market truth or as guaranteeing detection or completeness.

Customers must not upload malicious or unlawful APKs, or APKs they lack rights and authorization to test. Authorized third-party APK testing remains subject to Target Certification, applicable feature approval, and the Terms of Service. Lythe may scan, restrict, reject, or remove uploaded files where necessary to protect the Services, users, or third parties.

7. How We Share Information

We may disclose personal information as described below:

Authorized Lythe employees and persons contracted by Lythe may access Permitted Inputs, relevant Outputs and service records as necessary to provide the accepted work and any purchased manual bug verification, subject to confidentiality, least-necessary access, the DPA and any Data Approval. This does not authorize prohibited data or extend an approved purpose, recipient or retention period.

With Lythe affiliates, including between Lythe Inc. and Lythe Pte. Ltd., where necessary to operate, support, secure, administer, provide, or comply with obligations relating to the Services, subject to applicable law and applicable agreements.

With service providers and subprocessors that help us provide hosting, infrastructure, analytics, product analytics, session replay, AI infrastructure, payments, support, security, logging, communications, consent management, transcription, and other operational services. These providers may process device information, identifiers, page activity, feature usage, interaction events, and session replay data on Lythe's behalf.

With customer-authorized integrations, such as CRM, calendar, helpdesk, data warehouse, messaging, product analytics, design, transcription, storage, or workflow systems connected by the customer.

With customers, administrators, and authorized account users who control or manage the relevant workspace, agent, call, transcript, simulation, AI persona, report, upload, or workflow.

With professional advisors, including lawyers, auditors, insurers, accountants, and financial advisors.

With law enforcement, regulators, courts, or other parties where we believe disclosure is required by law, legal process, or necessary to protect rights, safety, security, or prevent abuse.

In connection with a merger, acquisition, financing, reorganization, due diligence process, asset sale, or similar corporate transaction, subject to appropriate safeguards.

With consent or at the direction of the relevant user or customer.

8. Subprocessors and Third-Party Services

The current provider disclosure identifies AWS, Cloudflare, Google Cloud Vertex AI (Gemini models), Vercel, Stripe, and PostHog for the operational functions and roles described in that list. Lythe contracts for and controls PostHog only for its landing-website analytics and replay. A PostHog integration inside the product, together with Mixpanel, Snowflake, Amplitude, FullStory, and Heap, is optional and customer-controlled; Fraser Simulation Studio functions without these integrations. They operate under the customer's provider account or agreement and

are not Lythe Subprocessors. Inclusion does not mean every provider receives every data category. See the Lythe Subprocessor List for processing details.

Lythe uses PostHog on its landing website for analytics, feature usage measurement, event analytics, debugging, and, where enabled after consent, session replay. PostHog may process device and browser information, identifiers, page activity, navigation paths, interaction events, and session replay data in accordance with Lythe's instructions, applicable agreements, and applicable law. Any PostHog integration inside the product is contracted and controlled by the customer.

We use Stripe for payment processing, billing, subscription management, invoicing, refund processing, fraud prevention, and related payment operations.

Lythe maintains a current Lythe Subprocessor List. That list is the authoritative current provider disclosure for Customer Personal Data processing and is updated, with notice where required, in accordance with the applicable customer agreement or Data Processing Addendum.

9. Data Retention

We retain personal information for as long as reasonably necessary to provide the Services, administer payments and refunds, comply with legal obligations, resolve disputes, enforce agreements, maintain security, prevent fraud and abuse, honor opt-outs and suppression requests, and support legitimate business purposes.

Retention periods may vary depending on the type of information, customer configuration, legal requirements, product settings, provider settings, and contractual commitments. Permitted conversation-derived information and separately approved real customer records and feedback, workflow logs, simulation inputs, AI persona outputs, evaluation reports, permitted uploaded materials, APK files, screenshots, product analytics events, session replay recordings, support records, billing and refund records, security logs, and consent records may have different retention periods. Landing-website session replay recordings and associated analytics data are retained according to Lythe's configured retention settings and are deleted or anonymized when no longer reasonably necessary for the purposes described in this Policy. Retention for a customer-controlled PostHog product integration follows the customer's PostHog configuration and agreement.

Customer-configurable retention applies only to settings actually available for the relevant data category. Deletion requests, backup handling, and any permitted legal retention remain subject to applicable law and the controlling DPA or customer agreement.

Where Lythe processes personal data on a customer's behalf under a DPA, that DPA governs deletion, return, retention, and backup handling. General retention descriptions in this Policy do not override those obligations.

10. Security

We use administrative, technical, and organizational safeguards designed to protect personal information against unauthorized access, loss, misuse, disclosure, alteration, and destruction. These safeguards may include access controls, encryption, logging, monitoring, authentication, vulnerability management, vendor review, and incident response procedures.

No system is completely secure. Customers are responsible for maintaining the confidentiality of account credentials, configuring access permissions appropriately, limiting access to workspaces and integrations, and promptly notifying us of suspected unauthorized access or security incidents.

11. International Data Transfers

Lythe may process and store personal data in countries other than the country where it was originally collected, including through Lythe affiliates, service providers, and subprocessors used to provide the Services. In particular, personal data may be processed between Lythe Inc. in the United States and Lythe Pte. Ltd. in Singapore where necessary to provide, support, secure, administer, or comply with obligations relating to the Services.

These countries may have data protection laws that differ from those in the individual's jurisdiction. Where required by applicable law, Lythe will implement appropriate safeguards for cross-border transfers, such as contractual protections, data processing agreements, standard contractual clauses, transfer assessments, or other recognized transfer mechanisms. You may request information about applicable international-transfer safeguards and a copy where available by contacting team@lythe.ai. Confidential information may be redacted while providing information required by applicable law.

12. Privacy Rights and Choices

Depending on the applicable law and the user's location, individuals may have rights to access, correct, delete, restrict, object to, or receive a copy of their personal information. Individuals may also have the right to withdraw consent, opt out of certain marketing communications, limit certain uses of sensitive personal information, opt out of sale, sharing, targeted advertising, or qualifying profiling, appeal certain request decisions, or lodge a complaint with a data protection authority.

To exercise an applicable privacy right, email team@lythe.ai and identify the right requested and the person's relationship with Lythe or a Lythe customer. Lythe may request information reasonably necessary to verify the requester's identity, authority, and jurisdiction. Authorized agents may submit requests where permitted by law, subject to verification of their authority and, where legally permitted, confirmation from the individual.

Lythe will respond within the period required by applicable law. Where an appeal right applies, the requester may appeal a denial by replying to Lythe's decision or emailing team@lythe.ai with "Privacy Appeal" in the subject line. Lythe will not unlawfully discriminate or retaliate against an individual for exercising an applicable privacy right.

If personal data is processed by Lythe on behalf of a customer, individuals should generally direct their requests to that customer. Lythe will assist customers in responding to requests as required by applicable law and applicable agreements.

Users may opt out of marketing emails by using the unsubscribe link or contacting us. Operational, billing, legal, and security messages may still be sent where necessary.

13. Cookies and Similar Technologies

Lythe may use cookies, pixels, local storage, SDKs, tags, server-side tracking, product analytics, session replay, and similar technologies to operate websites and Services, remember preferences, authenticate sessions, analyze usage, understand page and feature interactions, diagnose bugs and usability issues, improve performance, prevent fraud, measure campaigns, attribute conversions, and, where enabled, support retargeting or relevant advertising through third-party platforms.

Lythe does not currently sell personal data collected through cookies or similar technologies for monetary consideration. However, depending on the technologies used and applicable law, disclosure of identifiers or online activity to advertising partners for targeted or cross-context behavioral advertising may be treated as a "sale," "sharing," targeted advertising, or similar regulated activity.

Where required by applicable law, Lythe will obtain consent before using non-essential cookies or similar technologies and will provide required notices and choices to opt out of regulated sale, sharing, targeted advertising, or similar processing. Where required by applicable law, Lythe will honor recognized opt-out preference signals, such as Global Privacy Control, for the relevant browser or device.

PostHog analytics and session replay on Lythe's landing website are optional. Visitors must approve them through Lythe's consent controls before they are enabled and may reject or later withdraw consent through Cookie settings. Consent-dependent collection must not begin before consent or continue after withdrawal. Requests to delete previously collected personal data are handled under this Policy and applicable law. A PostHog integration inside the product is separately controlled by the customer under the customer's own PostHog account.

More information is available in the Lythe Cookie Policy.

14. Regional Privacy Disclosures

14.1 Singapore PDPA

Where Singapore's Personal Data Protection Act 2012 applies, Lythe Pte. Ltd., or the applicable Lythe entity handling personal data in connection with Singapore customers or individuals, will collect, use, disclose, and transfer personal data only in accordance with applicable consent, notification, purpose limitation, protection, retention, transfer, access, correction, accountability, and data breach notification obligations.

Individuals may contact Lythe's Data Protection Contact to request access to or correction of their personal data, subject to applicable legal exceptions.

14.2 European Economic Area, United Kingdom, and Switzerland

Where EEA or UK data protection law applies to Processing for which Lythe acts as controller, account administration and business support rely on legitimate interests in providing and administering Services to the customer organization; contract applies where the individual is themselves the contracting party. Business billing administration relies on legitimate interests in receiving and reconciling payment, and required financial records rely on applicable legal obligations. Service security and abuse prevention rely on legitimate interests in protecting the Services, customers and third parties, or a specific legal obligation where applicable. Optional PostHog analytics and replay on Lythe's landing website rely on consent. Marketing relies on consent where required, or otherwise on legitimate interests only where lawful, subject to applicable opt-out rights. Privacy-request handling and required compliance records rely on the applicable legal obligation. Customer determines the lawful basis for Customer Personal Data Processed on its behalf under the DPA. Where GDPR, UK GDPR or Swiss law applies, individuals may have rights of access, rectification, erasure, restriction, portability, objection and withdrawal of consent, subject to applicable conditions.

14.3 California and Other U.S. State Privacy Laws

Where applicable U.S. state privacy laws apply, individuals may have rights to know, access, correct, delete, or obtain a copy of personal information; opt out of sale, sharing, targeted advertising, or qualifying profiling; limit certain uses or disclosures of sensitive personal information; use an authorized agent; appeal certain request decisions; and receive equal service and pricing without unlawful discrimination for exercising those rights.

Lythe does not currently sell personal data for monetary consideration. However, where enabled, certain advertising or retargeting technologies may involve processing that is regulated as sale, sharing, targeted advertising, or similar activity under applicable law. Where required, Lythe will provide applicable notices, opt-out mechanisms, and recognition of opt-out preference signals, such as Global Privacy Control.

Requests and appeals may be submitted to team@lythe.ai using the process in Section 12. Lythe may verify identity, authority, and jurisdiction before completing a request. If Lythe processes personal information solely on behalf of a customer, the individual should direct the request to that customer, and Lythe will assist as required by applicable law and agreement. Rights remain subject to applicable definitions, thresholds, exceptions, and limitations.

15. Children

The Services are not directed to children under 13, and Lythe does not knowingly collect personal data directly from children under 13 through its general-purpose website, public demos, product onboarding flows, or Fraser Simulation Studio.

Customers must not use the Services for workflows involving children or minors without Lythe's prior written approval and all required rights, notices, consents, safeguards, and legal authority. Where Lythe becomes aware that personal data involving children or minors has been processed in violation of this Policy or applicable law, Lythe may restrict processing, suspend the relevant workflow, require remediation, or delete data where appropriate and legally permitted.

16. Customer Responsibilities

Customers are responsible for:

Providing legally required privacy notices to their users, leads, customers, employees, research subjects, business contacts, and other individuals.

Obtaining required rights, notices, consents and lawful bases for source materials; minimizing inputs and removing prohibited information; supplying only Permitted Inputs; and obtaining Data Approval before sending or exposing real customer records, feedback or conversation materials to Lythe.

Ensuring that data uploaded to or made available through the Services is accurate, lawful, authorized, and appropriate for the intended use.

Responsibly managing account access, customer-controlled integrations and systems, permissions and retention settings available to Customer, permitted inputs, requested scenarios and downstream use of reports. Lythe configures, operates, monitors and stops its own agents and simulations within the accepted scope and safeguards; Customer must provide genuine authority and required confirmations and promptly report concerns or request stopping.

Responding to privacy rights requests where the customer acts as the controller or business under applicable law.

Using the Services only in accordance with applicable law, Lythe's terms and policies, and applicable customer agreements.

17. Changes to This Policy

Lythe may update this Privacy Policy from time to time to reflect changes in the Services, data practices, subprocessors, product names, legal requirements, or business practices. Updated versions will be posted or otherwise made available to affected individuals and customers.

Material changes apply prospectively from the effective date stated in the updated Policy, subject to applicable law. We will notify affected individuals of material changes as required by law. Where a change requires consent, that consent is required before the relevant processing begins. Continued use alone does not constitute that consent.

18. Contact Us

Questions, requests, or concerns about this Privacy Policy or privacy practices relating to Lythe services may be directed to:

U.S. parent: Lythe Inc.

Registered address: 2209 Van Ness Avenue, San Francisco, CA 94109

Singapore subsidiary: Lythe Pte. Ltd.

Data Protection Contact: team@lythe.ai

Privacy requests: team@lythe.ai

The Lythe entity responsible for a customer's use of the Services is identified in the applicable Terms of Service, Order Form, customer agreement, or other written agreement.