

ERRUNDS Privacy Policy (British Columbia PIPA)

Effective date: June 1, 2026. This Privacy Policy explains how **Runner Technologies Inc.** (doing business as **ERRUNDS**, “ERRUNDS,” “we,” “us,” or “our”) collects, uses, discloses, retains, and protects personal information when Customers and Runners access or use the ERRUNDS Platform. The Platform is a marketplace application connecting individuals seeking everyday task assistance (“Customers” or “Clients”) with individuals offering to complete such tasks (“Runners”). This Privacy Policy is intended to align with British Columbia’s *Personal Information Protection Act* (PIPA), Canada’s federal private-sector privacy law where applicable (PIPEDA), and other applicable privacy laws. It forms part of the ERRUNDS Terms of Service and is incorporated by reference into the ERRUNDS Runner Agreement, ERRUNDS Customer Agreement, and Fees, Payments & Cancellation Policy.

1. Definitions

For purposes of this Privacy Policy: (a) **Platform** means the ERRUNDS website, mobile application(s), and related services; (b) **Customer** (also called Client) means a user who requests a task; (c) **Runner** means a user who accepts and performs a task; (d) **Personal information** has the meaning in PIPA and generally means information about an identifiable individual, and does not include business contact information; and (e) **User Content** has the meaning in the ERRUNDS Terms of Service.

2. Contacting Us / Privacy Officer

If you have questions, want to withdraw consent (where permitted), or want to request access to or correction of your personal information, please contact our Privacy Officer:

- **Privacy Officer:** Timiel Mintu
- **Email:** support@errunds-app.ca
- **Mailing address:** 69-1235 LaSalle Pl. Coquitlam BC, Canada V3B6T4

3. What We Collect and Why (Purposes)

We collect personal information only for purposes that a reasonable person would consider appropriate in the circumstances, and we use and disclose personal information only as described in this Privacy Policy, the Terms of Service, and as permitted or required by applicable law.

Category	Examples	Primary Purposes
Account information	Name, email address, phone number, password or login credentials, profile photo, selected role, and account settings.	Account creation, authentication, communications, fraud prevention, and Platform administration.
Identity verification	Government-issued identification information, age confirmation, address, selfie or verification status, and screening results where permitted by law.	Runner verification, Customer verification where required, safety, trust, fraud prevention, and legal compliance.
Payment and payout information	Limited payment instrument details, transaction records, payout status, task amounts, fees, refunds, chargebacks, and tax-related records.	Payment processing, Runner payouts, receipts, invoice, dispute review, chargeback handling, accounting, and compliance.

Task and communication information	Task descriptions, scheduled time, task address, access instructions, before/after photographs, messages, reviews, ratings, and support communications.	Task matching, task completion, dispute resolution, customer support, safety review, and Platform integrity.
Location, device, and usage information	Task address, live GPS location of the Runner while navigating and while performing the accepted task, device identifiers, app version, crash logs, and push notification identifiers.	For Customer to monitor the Runner location while enroute and during task performance only. Operating and improving the Platform, facilitating tasks, security monitoring, notification delivery, fraud prevention, and analytics.

3.1 Account and profile information

When you create or manage an account, we may collect information such as your legal name or registered business name, profile photo, email address, phone number, address (as applicable), login credentials, and account settings. We use this information to register and administer your account, support account security, provide Platform features, communicate with you, and promote transparency and accountability in the community.

3.2 Task information and communications

To facilitate tasks, we may collect information you provide in task requests or bids (for example, task category, description, photos you upload, preferred schedule, task location/address, access instructions, and other information reasonably necessary to complete the task). We also collect and store in-app messages, in-app call metadata, and other communications between Users within the Platform. We use this information to match Customers and Runners, confirm the Service Understanding for a task, provide customer support, administer cancellations/refunds/disputes, and maintain Platform safety and integrity.

3.3 Payments and transaction information

Payments are processed by our third-party payment processor (currently Stripe). We and/or the payment processor may collect transaction details (for example, amounts, dates/times, payout details, and limited payment instrument information as permitted by the payment processors services). We use transaction information to process payments and payouts, detect fraud, manage chargebacks, maintain required records, and provide receipts and support.

3.4 Identity verification and screening (where permitted)

Where permitted by applicable law, we may collect information to verify identity and support Platform safety, integrity, and fraud prevention. (for example, legal name, date of birth/age confirmation, address, and government-issued identification information, as applicable). Verification may be conducted through trusted third-party providers. Unless required by law or necessary for verification, we do not intend to store full images/copies of government-issued identification; we may retain limited verification details (such as confirmation status or reference tokens) as permitted by applicable privacy laws and our practices.

3.5 Usage, device, and log information

When you use the Platform, we may collect information about how you interact with it, such as IP address, device identifiers, approximate location derived from your device (if enabled), app events, pages/screens viewed, and crash logs. We use this information to operate the Platform, improve functionality, diagnose

technical issues, prevent fraud and abuse, and maintain security. We may use app infrastructure and analytics tools, such as Firebase, to support authentication, database services, crash reporting, push notifications, app performance monitoring, security, and Platform diagnostics.

3.6 Live Location During Active Task

During an active task, the Platform may collect, use, and display real-time or near real-time GPS location information from a Runner's and/or Customer's device, where enabled and permitted by device settings. This information is used to coordinate arrival, support task progress, promote safety, verify completion, and display task-related location details on the in-app map for the matched Customer and Runner. Live location sharing is intended to operate only while the task is active and should stop when the task is completed, cancelled, or otherwise ended. We may also process limited location-related technical data to operate maps, support navigation, provide routing and address lookup, prevent fraud, support safety reviews, resolve disputes, and maintain Platform integrity. We may use third-party location services, such as Google Maps Platform, for these purposes. Users can manage location permissions through their device settings, but disabling location access may limit certain Platform features or affect the ability to request, accept, perform, or verify tasks.

If we use cookies or similar technologies, we use them for functions such as authentication, preferences, security, and analytics. You may be able to manage certain tracking technologies through your device or browser settings but disabling them may affect Platform functionality.

4. Consent (Including Withdrawal)

Subject to limited exceptions under PIPA, we obtain your consent to collect, use, and disclose your personal information. Depending on the circumstances and the sensitivity of the information, consent may be expressed or implied (for example, by voluntarily providing information to create an account, request a task, accept a task, communicate in-app, or complete verification steps).

You may withdraw consent, subject to legal or contractual restrictions and reasonable notice. Withdrawing consent may limit our ability to provide the Platform or certain features (for example, you may not be able to request/accept tasks or receive payouts). To withdraw consent, contact the Privacy Officer using the contact information above.

5. How We Share Personal Information

We disclose personal information as reasonably necessary to operate the Platform and facilitate tasks, and as otherwise permitted or required by law. We do not sell personal information.

5.1 Sharing between Customers and Runners

To facilitate a task, we share certain information between Customers and Runners, such as name, profile information, task details, task location/address, task instructions, and communications needed to coordinate the task. Users are expected to use information received through the Platform only for task-related purposes and in compliance with applicable law and Platform policies. During an active task, we may also share live or near real-time location information between the matched Customer and Runner through the in-app map for task coordination, safety, arrival tracking, and completion verification.

5.2 Service providers

We may share personal information with service providers who perform services on our behalf, including payment processing, identity verification and screening, cloud hosting, database services, authentication and sign-in services, maps, geolocation, routing and address lookup services, app analytics, crash reporting, push notifications, fraud prevention, security monitoring, customer support, and communications tools for email, SMS, push notifications, and in-app calls. These providers may include services such as Stripe, Firebase, Google Maps Platform, Google Sign-In, Apple Sign-In, LiveKit, and identity verification providers used by ERRUNDS from time to time. Service providers are permitted to handle personal information only to provide services to us and must protect it through appropriate contractual and security safeguards.

5.3 Legal, safety, and compliance disclosures

We may disclose personal information where permitted or required by law, including responding to lawful requests, court orders, or regulatory inquiries; to protect the rights, property, and safety of ERRUNDS, our users, or the public; to investigate suspected fraud, security incidents, or violations of our Terms/policies; and to support dispute resolution processes. Where appropriate and permitted, we may also disclose information to assist in investigating complaints related to illegal activity or safety concerns.

5.4 Business transactions

If we are involved in a merger, acquisition, financing, reorganization, or sale of some or all our business or assets, personal information may be disclosed as part of that transaction, subject to PIPA and appropriate safeguards.

6. Access to and Correction of Personal Information

Subject to limited exceptions under PIPA, you may request access to your personal information and request correction of errors or omissions. To make a request, contact our Privacy Officer. We may need to verify your identity before responding. We aim to respond within the time required by PIPA and may charge fees only as permitted by PIPA (and we will generally notify you in advance if a fee applies).

7. Safeguards

We make reasonable security arrangements to protect personal information in our custody or under our control against risks such as unauthorized access, collection, use, disclosure, copying, modification, disposal, or similar risks. Safeguards may include administrative, technical, and physical measures appropriate to the sensitivity of the information, such as access controls, encryption where appropriate, logging/monitoring, secure development practices, and staff training.

8. Retention and Destruction

We retain personal information only as long as necessary to fulfill the purposes identified in this Privacy Policy, to provide the Platform, and as required or permitted by law. We may also retain information to establish, manage, or defend legal claims, enforce our agreements, resolve disputes, and maintain business records. When personal information is no longer required, we will destroy, erase, or anonymize it in a manner appropriate to the sensitivity of the information.

Task-related photographs, in-app task messages, and exact task addresses are retained only as long as reasonably necessary for active task performance, support, dispute handling, fraud prevention, legal compliance, and enforcement of Platform policies. Where configured for MVP operations, task-related photographs, chat messages, and exact addresses will be deleted from active systems after the task is completed, subject to limited retention for payment disputes, chargebacks, legal claims, account history,

security, and compliance. Basic transaction records, including task name, date, amount, status, and related account history, may be retained for longer periods as required or permitted by law and for legitimate business purposes.

9. Accuracy and User Rights

We make reasonable efforts to ensure personal information we use or disclose is accurate and complete, considering the purposes for which it is used. You are responsible for keeping certain account information accurate and up to date through your account settings.

Subject to applicable law, you may request access to personal information we hold about you, ask us to correct inaccurate information, request deletion of your account and associated personal information where available, or withdraw consent to certain processing where permitted. Some information may need to be retained for legal, security, fraud prevention, dispute resolution, accounting, or legitimate business purposes. Requests may be submitted through Platform account settings where available or by contacting the Privacy Officer.

9.1 Account Deletion Request

You may request deletion or deactivation of your ERRUNDS account through the Platform account settings where available, or by contacting the Privacy Officer using the contact information in this Privacy Policy. After receiving a request, we may need to verify your identity and confirm that there are no unresolved tasks, payments, disputes, safety reviews, chargebacks, fraud investigations, or legal obligations connected to the account.

Where deletion is available, we will delete, erase, or anonymize personal information that is no longer required for the purposes described in this Privacy Policy. Some information may be retained where required or permitted by law, including for legal compliance, tax and accounting records, payment processing, fraud prevention, safety, dispute resolution, chargebacks, enforcement of Platform policies, or legitimate business recordkeeping. Deleting an account may remove access to Platform features, task history, messages, receipts, earnings records, and support records, except where such information is retained as described in Section 8.

10. Service Providers and Cross-Border Processing

Some service providers may process or store personal information outside British Columbia or Canada, including in the United States or other jurisdictions where they or their sub processors operate. These providers may support services such as cloud hosting, authentication, app infrastructure, analytics, maps and location services, communications, payment processing, fraud prevention, and identity verification. When personal information is processed outside British Columbia, it may be subject to the laws of that jurisdiction and may be accessible to law enforcement, courts, or other authorities there. We take reasonable steps to require service providers to protect personal information through contractual, technical, and organizational safeguards appropriate to the sensitivity of the information.

11. Privacy Incidents / Breach Response

If we become aware of a privacy incident involving personal information, we will take reasonable steps to contain, investigate, and remediate it, and we will provide notices to affected individuals and/or regulators where required or where we determine it is appropriate in the circumstances.

12. Age Eligibility

The Platform is intended for users who are at least 19 years of age (or the legal age required in your place of residence). We do not knowingly collect personal information from individuals under 19 in British Columbia for Platform use. If you believe a minor has provided us with personal information, please contact the Privacy Officer.

13. Communications: Telephone Text, and In-App calls

The Platform may allow Customers and Runners to communicate through in-app voice or video calling features for task-related purposes. These in-app calls may be powered by third-party communications infrastructure providers, such as LiveKit. When you use in-app calling, we collect mic permission and call metadata to connect the task parties. We and/or our service providers may process call-related technical data, such as call participants, call time, duration, device/network information, connection quality, and other metadata needed to connect, secure, operate, troubleshoot, and improve the calling feature. ERRUNDS does not permit users to record calls without the prior consent of all participants and compliance with applicable law. Unless expressly disclosed in the Platform or required for safety, support, legal, or dispute-resolution purposes, ERRUNDS does not record or store the content of in-app calls. In-app calls should be used only for task-related communications between Customers and Runners.

We may use your contact information to send service-related communications (for example, confirmations, reminders, security alerts, and support messages) by email, phone, SMS, or push notifications, consistent with your account settings and applicable law. Where we monitor or record telephone calls for quality control or training, we will provide notice and choices as described in the Terms of Service.

14. Updates to this Privacy Policy

We may update this Privacy Policy from time to time. If we make material changes, we will provide notice through the Platform and/or by email, and we will update the effective date above. Continued use of the Platform after the effective date of an updated Privacy Policy constitutes acceptance of the updated policy, except where applicable law requires additional steps.

15. Governing Law and Relationship to the Complete Agreement

This Privacy Policy is governed by the laws of the Province of British Columbia and applicable federal laws of Canada, except to the extent that applicable law requires otherwise or preserves non-waivable rights. If there is a conflict between this Privacy Policy and another part of the ERRUNDS complete user agreement, the provision that is more specific to the subject matter will apply, subject to applicable law and any order-of-precedence clause in the Terms of Service or related agreement.

16. Acknowledgment and Consent

By creating an account, accessing or using the Platform, requesting or accepting a task, submitting verification or payment information, enabling location permissions, communicating through the Platform, or otherwise using ERRUNDS services, you acknowledge that you have had an opportunity to review this Privacy Policy and understand that ERRUNDS may collect, use, disclose, retain, and protect personal information as described in this Privacy Policy and as permitted or required by applicable law.

Where the Platform asks for express consent for specific features or types of personal information, such as live location sharing during an active task, identity verification, payment processing, push notifications, or other sensitive permissions, your selection or continued use of those features confirms your consent to the related collection, use, and disclosure of personal information for the purposes described in this Privacy Policy.

If you do not agree with this Privacy Policy, or if you withdraw consent where consent is required, you should not use the Platform or the affected features. Withdrawing consent may limit or prevent access to certain Platform services, including requesting tasks, accepting tasks, completing verification, using live location features, receiving payments or payouts, and accessing account-related services.