

ReziLink Software Inc. Privacy Policy

Version: 2026-08-25

Effective Date: August 25, 2026

Last Updated: August 25, 2026

Introduction

ReziLink Software Inc. ("ReziLink," "we," "us," or "our") provides a cloud-based platform that organizations (our **Customers**) can use to manage people, programs, services, applications, properties, volunteers, donors, forms, documents, payments, and communications. Our Customers may include nonprofit, charitable, public-sector, community, housing, and for-profit organizations. We are committed to protecting the privacy and confidentiality of personal information entrusted to us. This Privacy Policy describes how we collect, use, disclose, and protect personal information when you register or use the ReziLink platform, in compliance with the *Personal Information Protection and Electronic Documents Act (PIPEDA)* and other applicable Canadian privacy laws.

This Privacy Policy is effective as of August 25, 2026, and applies to all end-users of the ReziLink platform, including our Customers and individuals interacting with our Customers through the platform (such as staff, applicants, participants, volunteers, donors, clients, residents, and service recipients). By using the ReziLink platform, you acknowledge that you have read and understood this Policy.

Our Role as a Service Provider: In many cases, ReziLink acts as a service provider (or "data processor") on behalf of our Customers, who are the primary collectors and managers of your personal information (the "data controllers"). This means that the Customer organization you are engaging with determines why and how your information is used, and ReziLink processes that information solely to provide our services according to its instructions. We are responsible for safeguarding the personal information in our custody or control, and we have implemented internal policies and security measures to do so. We have also appointed a Privacy Officer to oversee our privacy practices and address any questions or concerns (see the **Contact Us** section below).

Personal Information We Collect

For the purposes of this Policy, "**Personal Information**" means any information about an identifiable individual. This includes details that can identify you directly or indirectly. Through the ReziLink platform, we may collect or handle various categories of personal information on behalf of our Customers, including:

- **Identification and Contact Information:** For example, full name, date of birth, home or mailing address, email address, telephone number, and similar contact details.
- **Account Credentials:** Information used to register or log in to the ReziLink platform, such as a username (which may be your email address) and a password (stored in a protected, hashed form).
- **Application and Program Information:** Details provided in application, intake, eligibility, enrolment, or service forms and related documents. Depending on the Customer and program, this may include household or family information, employment history, income and financial information, housing or service history, personal references, and other information the Customer requires to assess an application, provide a service, or administer a program.
- **Financial Information:** In connection with a Customer's programs, services, transactions, or reporting obligations, you or our Customer may provide financial details such as proof of income (pay stubs, tax returns, bank statements), credit information, budget or expense information, and related financial documents. This information is collected only as needed for the Customer's identified purposes.
- **Donor and Payment Information:** If a Customer enables donor-management or payment features, the platform may process donor profiles, donation and interaction history, campaign information, receipts, payment status, and transaction identifiers. Payment-card details are entered into the payment provider's systems; ReziLink does not intend to store complete card numbers or card security codes.

- **Volunteer Information:** If you are a volunteer, the platform may collect information related to your volunteer work. This can include your contact details, areas of interest or skills, availability, volunteer schedule and hours logged, and any credentials or background check information required for volunteering (e.g., certifications, references, or police record checks if applicable).
- **Participant, Household, Property, and Service Information:** Depending on the features a Customer uses, we may collect information about participants, household or family members, properties or units, occupancy or service agreements, and interactions or services provided. This can include addresses, household composition, program participation, service records, contributed hours, agreements, and related payment records where relevant.
- **Documents and Attachments:** Customers and users can upload documents to the ReziLink platform as part of applications or record-keeping. These documents may contain personal information - for example, identification documents (IDs, driver's licenses, passports), financial statements, employment letters, reference letters, signed agreements, photographs, and any other supporting materials. We collect and store these documents as provided, on behalf of our Customers.
- **Electronic Signature and Acknowledgement Information:** If a Customer requests an electronic signature, initials, or acknowledgement, ReziLink may collect the signature or mark, typed name, signing intent and attestations, consent to use electronic records, signing status, timestamps, document or form version and cryptographic hash, certificate or audit-trail data, IP address, and browser and device information. This evidence is collected and recorded on behalf of the Customer that requested the document or form. Not every form or document requires a signature. We also retain evidence that authenticated users were shown and acknowledged specific versions of this Privacy Policy.
- **Communications:** The platform may facilitate communications between you and a Customer organization. This includes messages or notes submitted through ReziLink, emails or notifications sent via the platform (for instance, confirmations of application submission, service updates, or volunteer activity notices), and any feedback or inquiries you send to us. Such communications may contain personal information like your email address, name, and the content of your correspondence.
- **Technical and Usage Information:** When you use the ReziLink platform, we collect certain technical data automatically to ensure the platform works correctly and to improve security. This data may include your IP address, device type, operating system, browser type, approximate geographic location (e.g. city or region), and timestamps of your logins or actions. We may also keep logs of user activity within the platform (such as changes made to a record or pages accessed), policy acceptance records, diagnostic information, and security events for audit, security, legal evidence, and troubleshooting purposes. This information is generally linked to your account and treated as personal information when it is identifiable to you.

We collect most personal information directly from you or through our Customers (for example, when you fill out a form or your program administrator enters data about you). In some cases, our Customers may import or integrate data from other sources into the platform (for instance, if they already have a list of applicants or volunteers). Regardless of source, this Policy covers how we handle the personal information once it is in the ReziLink system. We do not collect more information than is necessary for the purposes of providing our services and fulfilling the purposes described below. If we ever need to collect additional types of personal information or use it for new purposes, we will do so only with appropriate consent or as permitted by law.

Legal Basis for Collecting and Using Personal Information

ReziLink will only collect, use, and disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances, and in accordance with applicable law. Under PIPEDA and related laws, our legal bases for processing personal information typically include:

- **Consent:** In most cases, we rely on your consent (or the consent obtained by our Customer from you) to collect and handle your personal information. By providing information to the ReziLink platform - for example, by completing an application or intake form, registering for a program or volunteer role, or uploading documents - you are consenting to the collection, use, and disclosure of that information for the purposes identified at the time of collection and as outlined in this Privacy Policy. You (or the organization you are interacting with) may withdraw consent at any time, as described in the **Your Rights and Choices** section, subject to legal or contractual restrictions.

- **Contractual Obligations:** We also process personal information in order to fulfill our contractual obligations to our Customers. Customer organizations have agreements with ReziLink to use our software services for their programs, services, operations, and related data. When you provide information to a Customer through our platform, we handle that information as necessary to perform the contracted services. For example, processing may enable the Customer to evaluate an application, administer a program, maintain operational records, process a transaction, or record volunteer activity.
- **Legal Obligations:** In certain circumstances, we may need to collect, use, or preserve personal information to comply with a legal obligation. For instance, we may be required by law to retain records for a certain period, to produce information in response to a court order or subpoena, or to meet regulatory reporting requirements. In such cases, we will only process the minimum amount of information necessary and only for the purpose of complying with the law.
- **Other Permitted Grounds:** Occasionally, we may rely on other lawful bases as permitted by Canadian privacy laws. For example, PIPEDA allows organizations to collect or use personal information without consent for specific purposes such as investigations of a breach of an agreement or contravention of law, or in emergencies where someone's life, health, or security is at risk. ReziLink will only ever rely on such provisions in accordance with the law and will document any such processing.

If we ever need to process your personal information for a purpose that is not described in this Policy or not obvious at the time of collection, we will seek your consent or instruct our Customer to do so (unless the processing is otherwise authorized by law). We will not, without your consent, use your personal information for purposes that are materially different from the purposes for which it was collected.

How We Use Your Personal Information

ReziLink uses the personal information we collect strictly to operate, manage, and improve the platform and to support our Customers' programs, services, and operations. The main purposes for which we use personal information include:

- **Providing and Managing Services:** We use the information to deliver the features and functions of the ReziLink platform. This includes processing and displaying data as needed—for example, allowing a Customer to review application details, administer programs or services, manage people and properties, log volunteer activity, process donations or payments, and communicate with stakeholders. Your information is used to carry out the service or organizational function you expect.
- **User Accounts and Authentication:** Personal information is used to create and manage user accounts on the platform. For instance, we use your email and password to authenticate your login and to distinguish your profile and data from other users. We may also use contact information to verify your identity or to set up accounts when invited by a Customer.
- **Communication and Notifications:** We use contact information (like email addresses and phone numbers) to communicate with you regarding your use of the platform. Examples include confirmation emails when you register or submit information, notifications about an application, program, service, transaction, or event, updates from the Customer organization, and responses when you contact ReziLink Support. These communications may be automated through our system (e.g., reminders or alerts) or sent by our team or the Customer's team through the platform.
- **Electronic Records and Third-Party Service Integration:** ReziLink may present a form or document for native electronic signing and preserve evidence of the action, or a Customer may use a third-party integration such as Zoho Sign. Similarly, if you are enrolled in training through Zoho Learn, we use your user information to facilitate that experience. The information is used to carry out the function requested by the Customer and remains protected as described in this Policy.
- **Platform Improvement and Analytics:** We may analyze usage patterns and feedback (in aggregated and de-identified form whenever possible) to improve our services. Personal information (including technical usage data) helps us understand how users interact with the platform, which features are most used, and where improvements or new features might be needed. For example, we might look at how many users submit a certain form or which times of day the system is most active to optimize performance. These analyses are generally done on datasets that do not identify individuals; any insights that involve personal data are used internally by ReziLink and only for the purpose of enhancing the platform's functionality and user experience.

- **Customer Support and Operations:** If you reach out with a support question or if a Customer needs assistance related to your data, we will use your information to resolve the issue. This could involve reviewing the data in your account to troubleshoot a problem, helping a Customer update or correct information, or communicating with you to provide guidance. We also use information in day-to-day operations such as billing and account management for our Customers (which might include referencing a Customer's user list or storage usage, for example).
- **Security and Fraud Prevention:** We use personal and technical information to maintain the security of the platform and our users. For example, we may use your IP address and other technical signals to detect unusual account access patterns that could indicate fraudulent activity. Activity logs are used to audit actions and trace any unauthorized changes, which helps us prevent and respond to potential data breaches or misuse of the system. Personal information may be used to verify identity if we detect suspicious activity (e.g., confirming that a request to export data is legitimate).
- **Legal and Compliance Purposes:** We may use personal information as necessary to enforce our Terms of Service or agreements, comply with legal obligations, and address disputes. For instance, if there is an inquiry or audit by a regulatory body, we might need to use and provide relevant data to demonstrate compliance with laws or regulatory requirements applicable to ReziLink or the Customer. Similarly, if we need to pursue or defend a legal claim (for example, involving a security incident or contract dispute), we will use pertinent personal information as evidence and in communications with legal authorities or advisors.

We do **not** use personal information for any form of marketing or advertising to end-users, nor do we engage in profiling or automated decision-making that has legal or significant effects on individuals, except as necessary to deliver the services (such as automatically sorting applicants by certain criteria if that feature is used by a Customer, under their control). If our practices change in the future, we will update this Policy and, if required, seek appropriate consent.

Disclosure of Your Personal Information

ReziLink understands the importance of keeping your personal information private. We do not sell, rent, or trade your personal data to third parties for promotional purposes. We only disclose or share your information in the following circumstances, and always in accordance with this Policy and applicable laws:

- **To Your Customer Organization:** If you are using ReziLink as a staff member, applicant, participant, volunteer, donor, client, resident, service recipient, or other user, the information you provide is made available to the specific Customer that administers the form, document, transaction, program, service, or account. That Customer will use the information for its programs and operations and is responsible for its own privacy practices. **Information you submit through a Customer form or electronic-signature process is collected on behalf of that Customer.** You should consult the Customer's privacy notice or contact its administrator for details about its purposes and decisions.
- **Service Providers (Third-Party Processors):** ReziLink employs a number of trusted third-party service providers to perform certain functions on our behalf in order to operate the platform effectively. When we share your information with these providers, we do so under strict agreements that limit how they can use the information and require them to safeguard it in compliance with high security standards and Canadian privacy requirements. Key service providers and integrations include:
 - *Amazon Web Services (AWS) and Laravel Vapor:* We use AWS infrastructure and Laravel Vapor to host the core ReziLink application, databases, files, and backups in configured Canadian AWS regions. These providers process data as necessary to host and operate the service and are bound by confidentiality and security obligations.
 - *Zoho Sign:* A Customer may use Zoho Sign for third-party electronic signatures. In that case, the signer's name and email, document content, signing actions, and related evidence may be processed through the Customer's configured Zoho Sign service. ReziLink also offers native electronic signing that does not require sending the document to Zoho Sign.
 - *Zoho Learn:* Some Customers use Zoho Learn through ReziLink to provide training modules, educational content, or knowledge resources. We may share basic user information and relevant enrolment, progress, or completion information to enable that Customer-selected service.
 - *Payments, donations, communications, and diagnostics:* Depending on the features a Customer uses, Stripe or Zeffy may process payment or donation information; Mailgun or another configured email/SMS provider may deliver communications; and Sentry may process limited diagnostic and error information. These providers receive only information reasonably needed for the selected function and may process it in Canada or other jurisdictions under their own infrastructure and contractual safeguards.

- *Other Customer-Selected Tools:* A Customer administrator may enable another integration, export, or connected service. The Customer is responsible for selecting it, authorizing the transfer, and informing affected individuals where required. We assess ReziLink's service providers and update this Policy or notify Customers when a material provider change affects personal-information handling.
- **Within ReziLink (Authorized Personnel):** Within our company, personal information is accessible only to authorized employees or contractors who require access to do their jobs. For example, members of our technical support and engineering teams may access data when troubleshooting an issue or providing support to a Customer, but even then, they will only access the minimum necessary data. All ReziLink personnel are trained on privacy obligations and are bound by strict confidentiality agreements. We limit internal access to personal information on a need-to-know basis, controlled by role-based access permissions.
- **Legal Compliance and Protection:** We may disclose personal information outside of ReziLink and our service providers if we are required to do so by law, or if such disclosure is necessary to protect rights and safety. Situations where this might occur include:
 - Complying with legal processes or governmental requests: If we receive a court order, subpoena, warrant, or other lawful request for information, we may be obligated to disclose certain personal data to law enforcement, courts, or regulators. We will only do so after verifying the validity of the request and only provide information that is legally required. When permitted, we will notify the affected Customer (and individual, if appropriate) of such requests.
 - Enforcing our rights: We may disclose information as necessary to enforce our terms of service or agreements (for example, to collect overdue fees or to address a violation of our platform rules), or to protect the rights and property of ReziLink, our Customers, or others.
 - Preventing harm: If we believe that disclosure is necessary to prevent an act that could cause harm to individuals, property, or public safety (for example, to investigate fraud or security issues, or in the context of an urgent medical or safety situation), we may share information with the appropriate authorities or parties.
- **Business Transfers:** In the event that ReziLink undergoes a business transition such as a merger, acquisition by another company, consolidation, restructuring, sale of assets, or in the unlikely event of bankruptcy or receivership, personal information we have collected may be among the transferred assets. This means your data could be transferred to a successor or affiliate as part of that transaction. If such a transfer occurs, we will ensure that your personal information remains protected by measures equivalent to those set out in this Policy, and we will inform our Customers (and users, if appropriate) of the change in ownership or control of the personal information. The new entity will continue to be bound to respect your personal information in accordance with this Policy or will provide notice of any changes.
- **With Your Consent or Direction:** Aside from the scenarios above, we will share your personal information with third parties only if you (or our Customer, acting with your authority) expressly consent to or request such sharing. For example, if you ask us to transfer your data to another platform or service, or if you participate in a joint program involving a Customer and another service provider where you agree that information can be shared, we will do so as directed. Any additional disclosure of your personal information that is not covered by this Policy will be done with your knowledge and consent.

We reiterate that all third parties who may receive personal information as part of these disclosures are obligated to keep it secure and confidential. ReziLink does **not** permit any service provider to use or disclose personal data for any purpose other than to provide the services on our behalf or to comply with legal requirements. If you have questions about the third parties involved in handling your data, please feel free to contact us (see **Contact Us** section).

Data Residency and Cross-Border Processing

We understand that many Customers and users value Canadian data residency. ReziLink hosts its core application, database, files, and backups in configured Canadian AWS regions. However, a communication, payment, donation, diagnostics, support, electronic-signature, learning, or Customer-selected provider may process or allow authorized support access to limited information from another province, territory, or country.

Information processed outside Canada may be subject to the laws of that jurisdiction and may be accessible to its courts, law-enforcement agencies, or national-security authorities. ReziLink remains accountable for personal information transferred to service providers under its control and uses contractual, organizational, and technical measures designed to provide a comparable level of protection. Contact our Privacy Officer if you want information about processing relevant to a

particular ReziLink feature.

Data Security

ReziLink employs robust security measures to protect personal information against unauthorized access, alteration, loss, or disclosure. We recognize that the data our platform handles may be sensitive (for example, identity, financial, household, service, or housing-related information), and we treat it with the utmost care. Some of the key security practices we have implemented include:

- **Encryption:** All data exchanged with the ReziLink platform is encrypted in transit using industry-standard TLS (Transport Layer Security). You will see "https://" in our URLs, indicating a secure connection. Additionally, personal data stored in our databases and file storage is encrypted at rest. This means that even if someone were to gain unauthorized access to our storage, the data would be unreadable without the proper decryption keys.
- **Access Controls and Authentication:** We use role-based access control (RBAC) to ensure that both ReziLink staff and our Customers' users can only access the information they are authorized to see. Within our organization, only a limited number of trained personnel (for example, senior engineers or support staff) have access to production databases, and then only when necessary for support or maintenance tasks. Any such access is logged and monitored. Customer users are granted access permissions by their administrators based on their responsibilities—for instance, one user might manage volunteer records while another manages applications, services, properties, or payments. This layered permission system helps prevent unauthorized viewing or editing of personal information. All user accounts (both Customer administrators and end-user accounts) are protected by password authentication, and we strongly encourage the use of strong passwords and two-factor authentication (2FA) where available.
- **Employee and Contractor Training & Agreements:** Every ReziLink employee, and any contractor or partner who might assist us, is required to adhere to strict confidentiality obligations. We conduct background checks where appropriate and provide training to ensure everyone understands their responsibilities in protecting personal data. We have internal policies in place for data handling, and our staff must acknowledge and follow these policies. Access to personal data by staff is only granted on a need-to-know basis and requires management approval.
- **Network Security:** Our servers are protected by firewall systems and network security monitoring. We employ intrusion detection and prevention systems to guard against malicious access. For example, we have measures to protect against common web threats such as SQL injection, cross-site scripting, and DDoS (Distributed Denial of Service) attacks. AWS infrastructure provides additional security features and monitoring tools that we leverage to ensure the integrity of our environment. We also isolate our application environment such that Customer data is segregated, adding an extra layer of protection between different Customers' information.
- **Monitoring and Auditing:** We continuously monitor our platform for unusual activities or vulnerabilities. Security logs are maintained for critical systems and are reviewed periodically. If any suspicious activity is detected (such as repeated failed login attempts or an unrecognized device accessing an account), our systems will flag it for investigation or take automatic protective actions (like temporarily locking an account or blocking an IP address). We also regularly audit permissions and access roles to ensure that they are up-to-date and appropriate.
- **Security Testing and Updates:** ReziLink's development process incorporates security reviews and testing. We keep all software frameworks, libraries, and systems updated to the latest security patches. Periodically, we conduct vulnerability assessments and may engage independent security experts to perform penetration testing on our platform. Any identified issues are promptly addressed. We also have an incident response plan in place so that if a security incident were to occur, we can act quickly to mitigate it and notify affected parties as required by law.
- **Data Backup and Recovery:** We perform regular backups of our databases and critical systems to prevent data loss. These backups are encrypted and stored in secure Canadian locations (via AWS). In the event of a hardware failure or other issue, we have the ability to restore data from these backups to ensure continuity of service. Backup data is kept for a limited retention period and is automatically purged over time. We test our data recovery procedures to make sure that we can reliably restore information if needed.
- **Physical Security:** Although we rely on cloud infrastructure, the data centers housing our servers have rigorous physical security controls (guarded facilities, access badges, surveillance, etc.). AWS's Canadian data centers are certified to high industry standards for security and reliability.

- **Ongoing Commitment:** We know that cybersecurity threats continually evolve. ReziLink is committed to reviewing and improving our security measures on an ongoing basis. We maintain an up-to-date security policy and adapt our practices as new technologies and threats emerge. While no method of transmission over the Internet or electronic storage is 100% secure, we strive to exceed industry best practices to protect your personal information.

If you have any questions about the security of your data, or if you suspect any unauthorized access or breach related to the ReziLink platform, please contact us immediately at privacy@rezilink.com. We will investigate and notify affected individuals, Customers, and regulators where applicable law requires it.

Data Retention

We retain personal information only for as long as necessary to fulfill the purposes for which it was collected, or as required or permitted by law. Because ReziLink is a service provider to our Customers, our data retention practices are also designed to meet our Customers' needs. Here is how we approach retention:

- **Active Subscription Period:** While an organization remains an active Customer of ReziLink, we will retain personal data collected on its behalf in the platform. This allows the Customer to access historical information (for example, past applications, service or transaction records, volunteer contributions, or communications) as needed for its ongoing operations. Data is not deleted on a set schedule during an active subscription, unless the Customer chooses to delete it or requests us to do so.
- **Customer-Directed Deletion or Retention:** We provide our Customers with control over their data. Authorized Customer administrators can delete certain records or files through the platform interface. If an individual (such as an applicant or volunteer) asks to have their data removed, and the request is approved by the Customer, the Customer can delete the data or ask ReziLink to assist with deletion. We will comply with our Customer's instructions regarding deletion or retention of specific personal information, provided those instructions are in line with legal obligations. For example, if a volunteer withdraws consent and requests deletion of their profile, the Customer can remove their data from the platform, and that data will no longer be accessible in the system (aside from possible presence in backups, which will be handled as described below). On the other hand, a Customer might request extended retention of certain data (beyond the subscription) if required by a funding agreement or audit requirement, in which case we can accommodate that in accordance with the law.
- **End of Service / Termination:** The Customer's written agreement with ReziLink controls return and deletion of Customer Data. Under the current standard terms, access ends on termination and the Customer may request a one-time export during the following 30 days. ReziLink then retains an inactive archival copy for one year, after which remaining Customer Data is irreversibly deleted or anonymized unless law requires longer retention. If a Customer has a different written retention term, that term controls for that Customer.
- **Electronic Transaction and Policy Records:** Signed documents, signature audit trails, document hashes, and Terms or Privacy Policy acceptance records may be retained for the Customer's record-keeping needs and for ReziLink's legal, security, audit, and dispute-resolution purposes, subject to applicable law. These records may need to be retained after an account or related content is otherwise deleted.
- **Legal and Compliance Requirements:** Notwithstanding the above, we may retain certain personal information for a longer period if required to do so by law or legitimate business obligations. For example, laws relating to financial reporting, audits, or record-keeping might require retention of certain transaction records for a number of years. If ReziLink has to retain data for such purposes, we will ensure the data is archived securely and not used for any other purpose. Similarly, if there is an ongoing legal proceeding, investigation, or dispute, we may retain relevant information until it is resolved. In all cases, retained data remains subject to the protections of this Privacy Policy.
- **Aggregate or Anonymized Data:** In some cases, ReziLink may transform personal information into an aggregated or anonymized format for analytical and business purposes (for example, to calculate the total number of applications processed by the platform across all Customers, or to evaluate system performance metrics). Such aggregated data contains no personally identifying information and cannot be traced back to any individual. We may retain and use this non-personal data indefinitely to help us improve our services, understand trends, or publish reports, because it no longer contains personal information about any user.

After the applicable retention period has elapsed, and once there is no longer a need or legal obligation to keep personal information, we will ensure it is permanently and securely deleted or irreversibly anonymized. This includes erasing electronic records and securely disposing of any physical media if applicable. We also ensure that third-party processors who

might have received the data (such as backups on AWS or documents on Zoho Sign) delete the data from their systems in line with our retention practices.

Your Rights and Choices

As an individual whose personal information is held by ReziLink on behalf of our Customers, you have certain rights and choices regarding that information. ReziLink is committed to supporting our Customers in addressing these rights in accordance with PIPEDA and other applicable privacy laws. Your key rights include:

- **Right to Access:** You have the right to access the personal information about you that we hold. This means you can request confirmation of whether we are processing your personal data and receive an explanation of the types of information we have. You may also request a copy of your personal information. Upon written request and authentication of your identity, we will assist our Customer in providing you with your personal data under our control, typically within a reasonable timeframe. Please note that in a few situations, access might be restricted as permitted or required by law (for example, if providing access would reveal personal information about another individual or confidential business information). If we cannot provide certain information, we will inform you of the reasons (unless prohibited by law).
- **Right to Correction:** If you believe that any personal information we hold about you is incorrect, incomplete, or outdated, you have the right to request its correction or update. We encourage you to first reach out to the Customer organization with which you are associated, as it can often update your information directly within the platform. However, you can also contact ReziLink to request corrections. We will work with the Customer to verify and correct the information as needed. Keeping your information accurate and up-to-date is important to us; we rely on you and our Customers to notify us of any changes or errors. There is no cost to you for requesting a correction, and we will confirm once the correction is made.
- **Right to Withdraw Consent / Delete Information:** You have the right to withdraw your consent to the continued use or retention of your personal information, subject to legal or contractual limitations. In practice, this means you can request that your personal data be deleted from the ReziLink platform. For example, if you submitted an application but no longer wish to be considered, you can withdraw it and ask that your personal details be removed; or if you registered for a program or volunteer role and later change your mind, you can request deletion of the related profile. To make such a request, it is often most effective to contact the Customer organization that collected your information, as it has the authority to instruct deletion of data in our system. You may also contact ReziLink directly, and we will coordinate with the relevant Customer. Upon a valid deletion request, we will erase the information from the active database and confirm with you or the Customer once completed. Keep in mind that there are some instances where we or the Customer may need to retain certain information despite a deletion request—for example, for legal compliance (as described in the **Data Retention** section) or if the information is needed to resolve a dispute or protect legal rights. We will inform you if such a situation applies and will ensure that any retained data is only used for the required purpose. Withdrawing consent or requesting deletion may mean that the applicable services, programs, or benefits can no longer be provided to you.
- **Right to Data Portability:** Under emerging privacy norms, you may have the right to obtain a copy of the personal information you have provided to us, in a structured, commonly used and machine-readable format, and to transfer (or have transferred) that information to another service provider. While PIPEDA does not explicitly name this right as “portability,” ReziLink supports the principle of data portability. Practically, this could mean providing you (through the Customer or directly, as appropriate) with an export of your data—for example, a summary of application, program, service, transaction, or volunteer information—in a CSV or PDF format that can be used elsewhere. If you require such an export, please contact us or the relevant Customer organization, and we will do our best to assist, provided it does not infringe on the rights of others and is feasible to produce.
- **Right to Lodge a Complaint:** If you have a concern about how your personal information has been handled by ReziLink or within our platform, you have the right to file a complaint. We take privacy complaints very seriously. We encourage you to contact us at privacy@rezilink.com with your concerns, so we can work with you and the relevant Customer to resolve the issue. Our Privacy Officer will investigate all complaints and respond to you with the findings and any actions we will take to address the issue. If you are not satisfied with our response or believe we are not meeting our obligations under privacy laws, you have the right to escalate your complaint to the appropriate privacy regulator. In Canada, this is usually the Office of the Privacy Commissioner of Canada (for PIPEDA matters), or in some cases a provincial Privacy Commissioner or Ombudsperson (if provincial laws apply, such as in Quebec, British Columbia, or Alberta). We will provide you with information on how to contact the correct authority if needed.

Exercising Your Rights: Because ReziLink acts as a data processor for our Customers, if you want to exercise any of the above rights, the initial recommended step is often to contact the Customer organization that collected your data. It has direct administrative control over your information on our platform and can authenticate your request in context. For instance, a Customer can verify your identity and directly retrieve or correct records connected to your application, account, program, service, transaction, or other relationship. However, you are also welcome to contact ReziLink directly at privacy@rezilink.com for assistance. We will either address your request (if we have enough information to do so and it is within our authority) or work closely with the relevant Customer to help facilitate your request. We will not refuse any reasonable request to exercise rights without explaining the reason. In processing requests, we may need additional information from you to verify your identity and ensure the security of your data. There is typically no charge for making a request, though in rare cases where a request is unusually complex or repetitive, a minimal fee as allowed by law might be imposed (we would inform you in advance). Our goal is to be transparent and helpful in enabling you to exercise control over your personal information.

Contact Us

If you have any questions, concerns, or requests regarding this Privacy Policy or your personal information, please contact us. We are here to help.

- **Email:** privacy@rezilink.com
- **Mail:** Privacy Officer, ReziLink Software Inc., 77 Clearview Dr., Omemee, Ontario K0L 2W0, Canada

You may direct your message to the attention of our Privacy Officer. We will strive to respond to all inquiries promptly and courteously.

In your inquiry, please include your contact information and a clear description of your question or request regarding privacy. This will help our team address your concerns more efficiently.

Changes to this Privacy Policy

ReziLink may update this Privacy Policy from time to time to reflect changes in our practices, technologies, legal requirements, or for other operational reasons. When we update the Policy, we will revise the version and effective date at the top. For a material update, authenticated users will receive a prominent notice when they log in or during their next Platform session and a link to the complete updated Policy.

Users will be asked to select a separate, unchecked control acknowledging that the updated Privacy Policy was presented. ReziLink records the exact policy version and hash, account and Customer identifiers, timestamp, IP address, and browser information associated with the acknowledgement. An acknowledgement is not a waiver of privacy rights and is not blanket consent for a new or unrelated collection, use, or disclosure. Where applicable law requires consent for a new purpose or optional practice, that consent will be requested separately. Earlier policy versions and acknowledgement evidence may be retained for legal and audit purposes.

ReziLink Software Inc. is dedicated to protecting privacy and maintaining the trust of our users and Customers. Thank you for taking the time to read our Privacy Policy. If you have any further questions or need clarification on any aspect of this Policy, please reach out to us at privacy@rezilink.com.