

Rezidual A.I. Privacy Policy

Effective Date: 9/1/2026

1. Introduction

Arkipelago, LLC, d/b/a Rezidual A.I. (“Arkipelago,” “Rezidual A.I.,” “we,” “us,” or “our”), provides a residual and commission calculation and analytics platform for independent sales agents (1099 contractors) and independent sales organizations (“ISOs”) operating in the credit card and payments processing industry (the “Service”). This Privacy Policy explains what personal and business information we collect through the Service, how we use and share it, and the choices available to you. By creating an account, subscribing to, or otherwise using the Service, you agree to the practices described in this Privacy Policy.

This Policy applies to our website(s), web application(s), and any related tools we operate under the Rezidual A.I. name (collectively, the “Service”). It does not apply to third-party sites or services that we do not control, even if linked from the Service.

2. Who This Policy Covers

The Service is designed for business use by independent sales agents and ISOs in the payments industry, not for use by consumers regarding their personal, family, or household purposes. Most individuals who use the Service do so in a professional or business capacity. Some information we collect is nonetheless personal information about identifiable individuals (such as an agent’s name and contact details), and this Policy addresses that information accordingly.

3. Information We Collect

Contact and Account Information. Name, email address, phone number, business name, login credentials, and similar identifiers you provide when you register for or use the Service.

Financial, Commission, and Residual Data. Merchant processing volume, residual/commission splits, payout amounts, statement data, and related financial figures that you upload, input, or connect to the Service to generate calculations, reports, or analytics.

Business and Merchant Account Data. Information about the merchant accounts you or your ISO manage, including merchant identifiers, business names, processor/acquirer relationships, and related account-level data, to the extent you provide or connect it to the Service.

Inputs and Uploads Used for AI Features. Documents, statements, files, and text you submit to the Service’s AI-assisted or analytics features, and the outputs those features generate.

Usage and Technical Data. Log data, device and browser information, IP address, and usage patterns (e.g., features used, timestamps) collected automatically when you use the Service.

Payment Information. If the Service is offered on a paid subscription basis, billing details necessary to process payment, which may be collected and stored by a third-party payment processor rather than directly by us (see Section 5).

We do not intentionally collect or store full payment card numbers through the Service. Data retrieved from Connected Accounts (see Section 6) generally consists of processing volume, residual/commission splits, and merchant-level statement data rather than cardholder payment credentials.

4. How We Use Information

We use the information described above to: (a) provide, operate, and maintain the Service, including generating residual, commission, and analytics calculations; (b) process subscription payments and manage your account; (c) retrieve data from the processor platforms you connect to the Service, as described in Section 6; (d) communicate with you about the Service, including support, updates, and billing notices; (e) monitor, secure, and improve the Service, including detecting fraud, abuse, or technical issues; (f) comply with legal obligations and enforce our

Terms and Conditions; and (g) with your consent or as otherwise permitted, for any other purpose disclosed to you at the time of collection.

We do not sell your personal information, and we do not use the financial or merchant data retrieved through the Service to train AI or machine learning models, or share it across customer accounts.

5. How We Share Information

Service Providers. With vendors who perform services on our behalf, such as hosting, analytics, customer support, and payment processing, under contractual obligations to protect your information and use it only for the purposes we specify.

Connected Processor Platforms. See Section 6 below for detail on how information may be exchanged with third-party payment processing platforms you connect to the Service.

Legal and Safety. When required by law, regulation, legal process, or governmental request, or when we believe disclosure is necessary to protect the rights, property, or safety of Arkipelago, our users, or others.

Business Transfers. In connection with a merger, acquisition, financing, reorganization, or sale of assets, in which case information may be transferred as part of that transaction.

We do not sell personal information to third parties for monetary consideration, and we do not share your information for third-party advertising purposes.

6. Processor Integrations and Connected Accounts

To generate your reports, the Service may connect to third-party payment processing and reporting platforms — including but not limited to, without limitation, Fiserv, Global Payments, WorldPay, Maverick, and IRIS NMI — using credentials, API keys, or authorizations you provide or approve (“Connected Accounts”). Through these connections, we retrieve the data necessary to generate your residual, commission, and merchant reports, such as processing volume, residual/commission splits, and statement data.

We use access to Connected Accounts solely to generate your reports and calculations, and we do not use that access for any other purpose. Credentials and access tokens for Connected Accounts are encrypted at rest and in transit and are not shared with any party other than the applicable processor and the service providers described in Section 5. You may revoke a Connected Account’s access at any time by contacting us at support@rezidual.ai; we will process revocation requests promptly.

We do not control, and are not responsible for, the privacy or security practices of third-party processor platforms; please also review their own privacy policies and terms.

7. Data Security

We implement administrative, technical, and physical safeguards designed to protect the information we collect, including encryption in transit, access controls, and monitoring. However, no method of transmission or storage is completely secure, and we cannot guarantee absolute security. You are responsible for maintaining the confidentiality of your login credentials.

8. Data Retention

We retain personal and business information for as long as your account is active and as needed to provide the Service, comply with legal obligations, resolve disputes, and enforce our agreements. Retention periods for financial and commission data may be longer where needed to meet recordkeeping obligations.

9. Your Rights and Choices

Everyone who uses the Service does so in a business capacity — as an independent 1099 sales agent or on behalf of an ISO — rather than as an individual consumer using the Service for personal, family, or household purposes. This matters because most state comprehensive privacy laws only grant individual rights (such as access, correction,

deletion, or opt-out) to a “consumer,” a term that most of these laws — including Virginia, Colorado, Connecticut, and the majority of other states with comprehensive privacy laws — define to exclude anyone acting in a commercial or employment context. As a result, those laws generally do not grant rights over the business data you input into or generate through the Service.

California is a notable exception: California’s CCPA/CPRA extends certain privacy rights to individuals acting in a business capacity toward a company — including employees, job applicants, owners, directors, officers, and independent contractors — so agents or ISO representatives based in California may have rights under that law with respect to their own personal information.

To exercise any rights that may be available to you, contact us at support@rezidual.ai. We will respond in accordance with applicable law and will not discriminate against you for exercising these rights.

10. Children’s Privacy

The Service is intended for business use by adults (18 or older) acting as independent sales agents or on behalf of an ISO. We do not knowingly collect personal information from anyone under 18. If we learn we have done so, we will take steps to delete it.

11. Cookies and Similar Technologies

Cookies are small text files of information stored by your Internet browser on your device’s hard drive. We may use cookies and similar technologies to collect browsing data, keep track of your preferences and profile information, and collect general usage and volume statistical information. Our cookies do not collect personal or confidential information and are not spyware.

There are a number of different types of cookies; however, the Service uses:

Essential. These cookies are necessary to the core functionality of the Service and some of its features, such as access to secure areas.

Analytics and Customization. We use these cookies and technologies to analyze how the Service is accessed, used, or performing in order to improve your user experience and to maintain, operate, and continually improve the Service. For example, we use Google Analytics on the Service to collect page url/page title and user browser/system information, including browser type, referrer, language, java/flash support, IP address, and ad-serving data. For information on how Google Analytics collects and processes data, visit www.google.com/policies/privacy/partners/.

To opt out of Google Analytics, visit Google’s “How you can control the information collected by Google on these sites and apps” article, or install the [Google Analytics Opt-out Browser Add-on](#).

How to Manage Cookies. You have the right to decide whether to accept or reject certain cookies. You can set your browser not to accept cookies; however, in a few cases, some features of the Service may not function as a result. Essential cookies cannot be rejected, as they are strictly necessary to provide you with the Service.

12. Do Not Track and Global Privacy Control

Most web browsers and some mobile operating systems and applications include a Do Not Track (“DNT”) feature or Global Privacy Control (“GPC”) signal you can activate to signal a privacy preference regarding the collection of data about your online browsing activities. No uniform technology standard for recognizing and implementing DNT signals has been finalized, and we do not currently respond to DNT browser signals.

As described in Sections 4 and 5 above, we do not sell your personal information and do not share it for third-party advertising purposes. To the extent a browser or device you use to access the Service transmits a GPC signal, we will treat that signal, where applicable law requires it, as a request to opt out of any sale or sharing of your personal information, consistent with the choices described in Section 9.

13. International Users

The Service is intended for use within the United States by agents and ISOs operating in the U.S. payments industry.

14. Changes to This Policy

We may update this Privacy Policy from time to time. If we make material changes, we will notify you by posting the updated policy with a new effective date and, where required by law, provide additional notice. Your continued use of the Service after changes take effect constitutes acceptance of the revised Policy.

15. Contact Us

Questions or requests regarding this Privacy Policy can be directed to:

Arkipelago, LLC, d/b/a Rezidual A.I.

120 Donelson Pike, Ste 202

Nashville, TN 37214

support@rezidual.ai