

Privacy Policy

Rayson Technologies LLC

Effective Date: August 31, 2026

Last Updated: August 31, 2026

1. Introduction

Rayson Technologies LLC ("Rayson Technologies," "we," "us," or "our") is committed to protecting your privacy. This Privacy Policy ("Policy") describes the Personal Data we collect, how we use and share it, your rights and choices, and how you can reach us with privacy-related inquiries.

This Policy applies when you visit our website at asksenti.com (the "Site") or engage with our B2B software products, software development services, or consulting services (collectively, the "Services").

Please read this Policy carefully. If you do not agree with its terms, please discontinue use of the Site and Services.

2. Defined Terms

Throughout this Policy, the following terms have the meanings set out below:

- "Personal Data" means any information relating to an identified or identifiable individual, including data you provide to us and data we collect automatically during your interactions with our Site or Services.
- "Services" means our B2B SaaS software products, software development engagements, consulting services, and any related support or professional services we provide.
- "Client" means an individual, business, or organization that has entered into an agreement with Rayson Technologies to receive the Services.
- "Client Data" means Personal Data that a Client or its end users submit to, or that Rayson Technologies accesses or receives in connection with, the delivery of Services to that Client.
- "Data Controller" means the entity that determines the purposes and means of processing Personal Data. A Data Controller is also referred to as a "business" under US state privacy laws.
- "Data Processor" means the entity that processes Personal Data on behalf of a Data Controller. A Data Processor is also referred to as a "service provider" under US state privacy laws.
- "Subprocessor" means a third-party vendor engaged by Rayson Technologies to process Personal Data in connection with the delivery of Services.
- "you" means, depending on context, a Site visitor, a business contact, a Client representative, or an individual whose data Rayson Technologies processes as described in this Policy.

3. Scope and Roles

3.1 When We Act as a Data Controller

Rayson Technologies acts as a Data Controller when it determines the purposes and means of processing Personal Data, including:

- Personal Data collected from visitors to asksenti.com
- Contact and business information provided by prospects, partners, and Client representatives
- Data processed for our own internal business operations (e.g., marketing, finance, legal compliance)

3.2 When We Act as a Data Processor

Rayson Technologies acts as a Data Processor when processing Client Data on behalf of our Clients. This occurs across our lines of business:

- **SaaS products:** Our software stores, processes, and transmits data belonging to Clients and their end users
- **Software development:** We may build, configure, or operate systems that handle Client end-user data
- **Consulting engagements:** We may access Client systems or databases, or receive data exports or files from Clients

In these cases, the Client is the Data Controller. We process Client Data only in accordance with the Client's instructions and the terms of our applicable agreement. This Policy does not govern Rayson Technologies' processing of Client Data in its capacity as a Data Processor; the relevant Client's privacy policy governs the rights of their end users.

This Policy does not apply to the employment or personnel practices of Rayson Technologies.

Rayson Technologies is headquartered in the United States and provides its Services to business customers in the United States and, where we agree to do so, in the European Union, the United Kingdom, and other jurisdictions. Where we process the Personal Data of individuals located outside the United States, we do so in accordance with the data protection laws applicable to that processing, and we apply appropriate safeguards to any cross-border transfer of Personal Data, including transfers to the United States.

4. Personal Data We Collect

4.1 Information You Provide to Us

We collect Personal Data you voluntarily provide, including:

- **Contact information:** Name, business email address, phone number, job title, and company name
- **Communications:** Messages, inquiries, feedback, or other content you send us via forms, email, or other channels
- **Contractual and transactional information:** Information necessary to enter into, perform, or administer agreements with you or your organization

- **Account information:** Credentials and profile information you provide when accessing our products or portals

4.2 Information Collected Automatically

When you visit our Site, we may automatically collect:

- **Usage data:** Pages visited, time spent on pages, links clicked, and referring URLs
- **Device and browser information:** Browser type and version, operating system, device type, screen resolution, and language settings
- **Network information:** IP address and approximate geographic location derived from your IP address
- **Cookies and similar technologies:** As described in Section 6 below

4.3 Information from Third Parties

We may receive Personal Data about you from third parties, including:

- Business contact enrichment providers (e.g., firmographic or contact data appended to leads)
- Referral partners or resellers who refer you to our Services
- Publicly available professional sources (e.g., company websites, professional directories)

4.4 Information We Do Not Intentionally Collect

We do not intentionally collect sensitive Personal Data from Site visitors or business contacts. This includes, but is not limited to:

- Social Security numbers or government-issued identification numbers
- Financial account details or payment card numbers
- Health, medical, or genetic information
- Biometric data used for identification
- Racial or ethnic origin, political opinions, religious or philosophical beliefs, or sexual orientation

If you inadvertently provide any such information to us, please contact privacy@rayson-tech.com so we can promptly delete it. If a specific Service requires collection of sensitive data, we will clearly inform you of the purpose and obtain any required consent before doing so.

Note: In our capacity as a Data Processor on behalf of Clients, we may process sensitive data that Clients submit through our Services. In those cases, the Client is responsible for ensuring the lawful basis for that processing, and our Data Processing Agreement governs our handling of such data.

5. How We Use Personal Data

5.1 Purposes and Legal Bases

We use Personal Data for the following purposes:

Purpose	Legal Basis
Respond to inquiries and provide information about our Services	Legitimate interest / pre-contractual necessity
Enter into, perform, and administer contracts and Client engagements	Contractual necessity
Operate, maintain, and improve our Site and Services	Legitimate interest
Send administrative communications (service updates, security notices)	Contractual necessity / legitimate interest
Send marketing communications about our Services	Legitimate interest (with opt-out right)
Comply with legal obligations and enforce our agreements	Legal obligation / legitimate interest
Protect the security and integrity of our systems and Services	Legitimate interest
Conduct internal analytics and business planning	Legitimate interest

We do not sell your Personal Data to third parties, and we do not use it for automated decision-making that produces legal or similarly significant effects on individuals.

6. Cookies and Tracking Technologies

Our Site uses cookies and similar tracking technologies to operate, analyze, and improve Site functionality. These technologies may include:

Types of cookies we use:

- **Strictly necessary cookies:** Required for the Site to function. These cannot be disabled.
- **Analytics cookies:** Help us understand how visitors interact with the Site (e.g., pages viewed, traffic sources, session duration).
- **Preference cookies:** Remember your settings, language, and display preferences.
- **Marketing cookies:** Used where appropriate notice has been provided to track engagement and enable more relevant communications.
- **Web beacons and pixel tags:** Tiny graphic elements or scripts embedded in web pages or emails that track whether content has been accessed or an email has been opened.
- **Analytics tools:** Third-party software (such as Google Analytics or similar services) that collects information about how you interact with our Site, including pages visited, session duration, and navigation paths.
- **Log files:** Automatically recorded data about your device and usage upon each visit, including IP address, browser type, pages viewed, and timestamps.
- **Local and session storage:** Technologies that store data locally on your device to improve performance and remember preferences across or within sessions.

You may control or disable non-essential cookies through your browser settings. Most browsers allow you to refuse cookies, delete existing cookies, or be notified before a cookie is set. Disabling

certain cookies may affect Site functionality. We honor browser-level Global Privacy Control (GPC) signals where technically feasible.

7. How We Share Personal Data

We do not sell or rent Personal Data. We may disclose Personal Data in the following circumstances:

- **Subprocessors and service providers:** We engage third-party vendors to assist in operating our Site and delivering our Services, including cloud hosting providers, analytics platforms, CRM tools, email service providers, and security vendors. Each Subprocessor is bound by contractual data protection obligations at least as protective as those described in this Policy. A current list of Subprocessors is available upon written request to privacy@rayson-tech.com.
- **Professional advisors:** Lawyers, accountants, auditors, and insurers, subject to confidentiality obligations.
- **Business transfers:** In connection with a merger, acquisition, restructuring, or sale of assets, we will provide reasonable advance notice and ensure the successor is bound by obligations consistent with this Policy.
- **Legal requirements:** When required by applicable law, regulation, court order, or governmental request, we will disclose only the minimum Personal Data necessary and, where permitted, will notify you in advance.
- **Protection of rights:** To protect the rights, property, or safety of Rayson Technologies, our Clients, employees, or others, or to detect, investigate, or prevent fraud or security incidents.
- **With your consent:** In any other circumstance where you have provided explicit prior consent.
- **Aggregated or de-identified data:** We may share aggregated or de-identified information that cannot reasonably be used to identify you, without restriction.

8. Data Retention

We retain Personal Data for as long as necessary to fulfill the purposes for which it was collected, support ongoing business relationships, and comply with applicable legal obligations. The following general schedules apply:

Data Type	Retention Period
Prospect and marketing contact data	3 years from last interaction, or until opt-out
Client contact and account data	Duration of engagement plus 5 years
Contract and transaction records	7 years
Website analytics and log data	13 months rolling
Security and access logs	1 year rolling, or longer if required for an active investigation

Client Data processed as a Data Processor	As specified in the applicable Client agreement or DPA
---	--

When Personal Data is no longer required, we dispose of it securely through deletion or de-identification. Where immediate deletion is not technically feasible, we restrict further access and processing until deletion is possible.

9. Data Security

Rayson Technologies maintains a formal security program designed to protect Personal Data against unauthorized access, disclosure, alteration, and destruction. Our safeguards include:

- **Encryption:** Personal Data is encrypted in transit using TLS and, where appropriate, at rest using industry-standard encryption.
- **Access controls:** Access to Personal Data is restricted on a need-to-know basis using role-based access controls. Multi-factor authentication is required for systems containing Personal Data.
- **Monitoring and logging:** We maintain audit logs of access to sensitive systems and monitor for anomalous or unauthorized activity.
- **Vulnerability management:** We conduct periodic security assessments, including vulnerability scanning, with documented remediation procedures.
- **Vendor management:** Subprocessors are assessed for security practices prior to engagement and subject to contractual security obligations.
- **Incident response:** We maintain a documented incident response plan. In the event of a confirmed security incident affecting Personal Data, we will take all steps to notify affected Clients and individuals as required by applicable law and our contractual obligations, without undue delay.
- **Employee training:** All employees with access to Personal Data receive security awareness training upon onboarding and on a recurring annual basis.

No method of electronic transmission or storage is 100% secure. If you have reason to believe that your Personal Data has been compromised, please contact us immediately at privacy@rayson-tech.com.

10. Data Processing on Behalf of Clients

When Rayson Technologies processes Client Data as a Data Processor, the following principles govern that processing:

- **Instructions-based processing:** We process Client Data solely in accordance with the documented instructions of the applicable Client, as set out in the relevant agreement (Master Services Agreement, Statement of Work, or standalone Data Processing Agreement).
- **Data Processing Agreements:** All engagements involving the processing of personal data are governed by a Data Processing Agreement (DPA) or equivalent data protection terms. Clients may request our standard DPA by contacting privacy@rayson-tech.com.

- **Subprocessors:** We engage Subprocessors only where necessary to deliver the Services, and ensure each is bound by data protection obligations consistent with our own. We will inform Clients of any intended changes to our Subprocessor list that may affect Client Data processing, and provide a reasonable opportunity to object prior to those changes taking effect.
- **Confidentiality:** All Rayson Technologies personnel authorized to process Client Data are subject to confidentiality obligations.
- **Data subject requests:** Where a Client's end user submits a privacy rights request to Rayson Technologies, we will promptly forward it to the applicable Client and provide reasonable assistance to enable the Client to fulfill its legal obligations.
- **Security incidents:** In the event of a confirmed or reasonably suspected security incident affecting Client Data, we will notify the applicable Client without undue delay and in accordance with our contractual obligations, and will cooperate with the Client's response and investigation.
- **Return and deletion:** Upon termination of a Services engagement, we will return or securely delete Client Data as directed by the Client and as specified in the applicable agreement.

If you are an individual whose Personal Data has been processed by Rayson Technologies on behalf of one of our Clients, please direct your privacy inquiries to the relevant Client organization.

11. Third-Party Links

Our Site may contain links to third-party websites or services provided for convenience only. Rayson Technologies does not endorse and is not responsible for the privacy practices or content of those third-party sites. We encourage you to review the privacy policies of any third-party sites before providing your information.

12. Children's Privacy

Our Site and Services are directed at business professionals and are not intended for individuals under the age of 13 (or such higher age as required by applicable law in your jurisdiction). We do not knowingly collect Personal Data from children. In compliance with the Children's Online Privacy Protection Act (COPPA) and similar laws, we do not solicit or accept Personal Data from anyone we know to be under 13 years of age.

If you are a parent or guardian and believe that your child has provided us with Personal Data without your consent, please contact us at privacy@rayson-tech.com. If we learn that we have inadvertently collected Personal Data from a child under 13 without verifiable parental consent, we will take prompt steps to delete that information from our systems.

13. Your Privacy Rights and Choices

Depending on your relationship with us and applicable law, you may have the following rights with respect to Personal Data we hold about you as a Data Controller:

- **Access:** Request a copy of the Personal Data we hold about you
- **Correction:** Request that we correct inaccurate or incomplete Personal Data
- **Deletion:** Request that we delete your Personal Data, subject to legal retention requirements
- **Portability:** Request that we provide your Personal Data in a structured, machine-readable format
- **Opt-out of marketing:** Unsubscribe from marketing communications at any time via the unsubscribe link in any marketing email, or by contacting privacy@rayson-tech.com

If you are located in the European Economic Area, the United Kingdom, or Switzerland, additional rights apply to you, as described in Section 16 (International Users: EU and UK Privacy Rights).

To exercise any of these rights, please contact privacy@rayson-tech.com with a description of your request and sufficient information for us to verify your identity. We will respond within 45 days, or as otherwise required by applicable law. We will not discriminate against you for exercising your privacy rights.

Note: If your Personal Data is processed by Rayson Technologies as a Data Processor on behalf of a Client, please direct your request to that Client, as they are the Data Controller responsible for that data.

14. Nevada Privacy Notice

Rayson Technologies does not sell "covered information" as defined under Nevada Revised Statutes Chapter 603A and does not engage in the sale of Personal Data for monetary consideration. Nevada residents may nonetheless submit opt-out requests to privacy@rayson-tech.com. We will respond within 60 days as required by Nevada law.

15. Complaints and Supervisory Authorities

If you have concerns about our privacy practices, we encourage you to contact us first using the details in Section 18 below so we can work to resolve your concern directly.

You may also have the right to lodge a complaint with a relevant supervisory authority. Applicable contacts include:

- **California residents:** California Privacy Protection Agency (CPPA) at cppa.ca.gov, or the California Attorney General at oag.ca.gov.
- **Nevada residents:** Nevada Attorney General's Office at ag.nv.gov.
- **Federal (US) matters:** Federal Trade Commission (FTC) at ftc.gov.

16. International Users: EU and UK Privacy Rights

This section applies when Rayson Technologies acts as a Data Controller of Personal Data relating to individuals located in the European Economic Area (EEA), the United Kingdom, or Switzerland. Where Rayson Technologies processes such Personal Data on behalf of a Client as

a Data Processor, the Client's privacy notice and our Data Processing Agreement govern, as described in Sections 3 and 10.

16.1 Legal Bases for Processing

When the EU General Data Protection Regulation (GDPR) or the UK GDPR applies, we process Personal Data only where we have a lawful basis to do so. Depending on the context, our lawful bases are:

- **Consent:** where you have given consent to processing for a specific purpose, which you may withdraw at any time.
- **Contract:** where processing is necessary to enter into or perform a contract with you or your organization.
- **Legal obligation:** where processing is necessary to comply with a legal obligation to which we are subject.
- **Legitimate interests:** where processing is necessary for our legitimate interests, such as operating, securing, and improving our Site and Services and pursuing business development, provided those interests are not overridden by your rights and freedoms.

Where we rely on legitimate interests, you may contact us for more information about that assessment. The purposes for which we use Personal Data and their corresponding bases are summarized in Section 5.

16.2 Your Rights in the EEA, UK, and Switzerland

If the GDPR or UK GDPR applies to our processing of your Personal Data as a Data Controller, you have the following rights, subject to the conditions and exemptions provided by applicable law:

- **Access:** obtain confirmation of whether we process your Personal Data and a copy of that data.
- **Rectification:** have inaccurate or incomplete Personal Data corrected.
- **Erasure:** have your Personal Data deleted in certain circumstances.
- **Restriction:** request that we restrict our processing of your Personal Data in certain circumstances.
- **Objection:** object to processing based on our legitimate interests, and object to processing for direct marketing at any time.
- **Portability:** receive the Personal Data you provided to us in a structured, commonly used, machine-readable format, and have it transmitted to another controller where technically feasible.
- **Withdraw consent:** withdraw your consent at any time where we rely on consent, without affecting processing carried out before withdrawal.
- **Automated decisions:** not be subject to a decision based solely on automated processing that produces legal or similarly significant effects. We do not engage in such automated decision-making.
- **Lodge a complaint:** complain to a supervisory authority, as described in Section 16.4.

To exercise any of these rights, contact privacy@rayson-tech.com. We will respond within the timeframe required by applicable law, generally within one month.

16.3 International Data Transfers

Rayson Technologies is located in the United States and may process and store Personal Data in the United States and in other countries whose data protection laws may differ from those in your jurisdiction. Where we transfer Personal Data from the EEA, the United Kingdom, or Switzerland to a country that has not received an adequacy decision, we rely on appropriate safeguards, including the European Commission's Standard Contractual Clauses and the UK International Data Transfer Addendum, together with supplementary measures where required. You may request a copy of the relevant safeguards by contacting privacy@rayson-tech.com.

16.4 EU and UK Representative and Supervisory Authorities

Where required by Article 27 of the GDPR or the UK GDPR, Rayson Technologies will appoint a representative in the European Union and the United Kingdom and will identify that representative in this Policy. If you are located in the EEA, the United Kingdom, or Switzerland, you have the right to lodge a complaint with your local supervisory authority. In the United Kingdom, this is the Information Commissioner's Office (ICO) at ico.org.uk.

17. Changes to This Privacy Policy

We may update this Policy periodically to reflect changes in our practices, technology, or legal requirements. When we make changes, we will revise the "Last Updated" date at the top of this page. For material changes, we will provide prominent notice on our Site or by direct communication to affected individuals or Clients at least 30 days prior to the change taking effect. Your continued use of the Site or Services after the effective date constitutes acceptance of the updated Policy.

18. Contact Us

If you have questions, concerns, or requests related to this Privacy Policy or our privacy practices, please contact us at:

Rayson Technologies LLC

Attn: Privacy & Legal

4910 Corporate Drive NW, Suite F

Huntsville, AL 35805

privacy@rayson-tech.com

rayson-tech.com