RESIN8 DATA PROCESSING AGREEMENT

1. PURPOSE AND REGULATORY SCOPE

This Data Processing Agreement governs Resin8's collection, use, storage, and processing of personal information in connection with our industrial equipment marketplace platform and related services. This Agreement applies to all users regardless of location and addresses compliance requirements under multiple data protection frameworks including the European Union General Data Protection Regulation, Canada's Personal Information Protection and Electronic Documents Act, the Texas Data Privacy and Security Act, and other applicable data protection laws.

This Agreement supplements and should be read in conjunction with our User Agreement, Privacy Policy, and any applicable specialized service agreements. In the event of conflicts between this Agreement and other documents, the more protective privacy provision shall govern to ensure maximum compliance with applicable data protection requirements.

We are committed to implementing appropriate technical, organizational, and administrative safeguards to protect personal information while enabling effective marketplace operations and artificial intelligence development that enhances user experience and platform security.

2. DEFINITIONS AND DATA PROTECTION ROLES

Personal information means any information relating to an identified or identifiable individual including names, contact details, identification numbers, location data, online identifiers, and factors specific to physical, physiological, genetic, mental, economic, cultural, or social identity. This definition encompasses both directly identifying information and information that becomes identifying when combined with other available data.

We act as a data controller when determining the purposes and means of personal information processing for platform operations, account management, transaction facilitation, security monitoring, fraud prevention, business analytics, artificial intelligence development, and regulatory compliance activities. In these contexts, we independently determine how and why personal information is processed.

When we act as a data processor on behalf of sellers, we process personal information only according to documented seller instructions and maintain separate technical and organizational measures to prevent commingling of controller and processor data. Sellers acknowledge that they remain the data controller for buyer information shared during transactions and bear responsibility for ensuring lawful processing bases for such sharing.

Users act as data controllers for their own business information, customer data, and any personal information they collect or process in connection with their business activities. Users also serve as data subjects when their own personal information is processed by us or other platform participants.

3. LAWFUL BASIS AND PROCESSING PURPOSES

We process personal information based on multiple lawful grounds depending on the specific processing activity and applicable legal framework:

Contract performance serves as the lawful basis for processing necessary to provide marketplace services, facilitate transactions, manage user accounts, coordinate payment processing, and fulfill our contractual obligations to platform users (GDPR Article 6(1)(b))

Legitimate business interests justify processing for platform security and fraud prevention, business analytics and performance measurement, artificial intelligence development and improvement, customer support and user experience enhancement, regulatory compliance and legal obligation fulfillment, and business operations including accounting, risk management, and strategic planning (GDPR Article 6(1)(f))

Legal obligations require processing for tax compliance and reporting, export control and sanctions screening, anti-money laundering verification, regulatory reporting and cooperation with authorities, court orders and legal process compliance, and industry-specific regulatory requirements applicable to marketplace operations (GDPR Article 6(1)(c))

Consent serves as the lawful basis for processing related to marketing communications, optional feature utilization, AI training for non-essential purposes, third-party integrations selected by users, and any processing activities that require explicit user authorization under applicable law (GDPR Article 6(1)(a))

4. CATEGORIES OF PERSONAL INFORMATION PROCESSED

User account information includes business contact details, individual contact persons, authentication credentials, account preferences and settings, verification documents and business credentials, billing and payment information, and communications preferences and marketing consents.

Transaction and marketplace data encompasses equipment listing details and specifications, purchase orders and transaction documentation, payment processing information, shipping and logistics coordination, user communications and messaging, dispute resolution records, and transaction outcome and performance data.

Technical and usage information covers platform interaction logs and analytics, device and browser characteristics, IP addresses and network information, session data and authentication tokens, security monitoring and fraud detection data, search queries and content interaction patterns, and performance metrics and error reporting.

Artificial intelligence training data includes listing content and images, search behavior and interaction patterns, transaction patterns and outcomes in aggregated form, user feedback and platform usage optimization data, and market trend and analytics information derived from platform activities.

5. INTERNATIONAL DATA TRANSFERS AND SAFEGUARDS

Personal information may be transferred to and processed in multiple jurisdictions including the United States where our primary operations are located, Canada where our engineering teams are based, and other countries where our service providers, payment processors, or business partners operate.

We implement appropriate safeguards for international data transfers including Standard Contractual Clauses approved by the European Commission for transfers from the European Union, adequacy decision frameworks where available for specific country destinations, binding corporate rules for transfers within our corporate group, and supplementary measures including encryption, access controls, and contractual protections for transfers to countries without adequate data protection frameworks.

Users consent to international data transfers necessary for platform operation and service provision by using our platform and agreeing to this Agreement. We provide additional information about specific transfer destinations and safeguards in our Privacy Policy and make such information available upon request.

We regularly monitor international data protection developments and adjust our transfer mechanisms as necessary to maintain compliance with evolving legal requirements and regulatory guidance from competent data protection authorities.

6. ARTIFICIAL INTELLIGENCE AND AUTOMATED PROCESSING

Our platform extensively utilizes artificial intelligence and machine learning systems for equipment classification and categorization, pricing analysis and market recommendations, fraud detection and security monitoring, content moderation and policy enforcement, user matching and recommendation systems, search functionality and results optimization, and platform performance monitoring and improvement.

AI development and training activities use personal information in both individually identifiable and anonymized forms depending on the specific application and legal requirements. We implement technical measures to minimize privacy risks in AI training including data minimization to use only necessary information, anonymization and pseudonymization where technically feasible, access controls limiting personnel exposure to training data, retention controls for AI training datasets, and bias monitoring and mitigation procedures.

Automated decision-making occurs in specific circumstances including fraud detection systems that may flag suspicious activities or transactions, content moderation algorithms that review listings for policy compliance, recommendation systems that suggest relevant equipment or business connections, and risk assessment systems that evaluate transaction or user risk factors.

Users have the right to request human review of automated decisions that significantly affect their platform experience, business relationships, or account status. Such requests must be submitted through our designated channels and will be processed according to applicable legal timeframes and requirements.

7. USER RIGHTS AND REQUEST PROCESSING

Universal rights available to all users include the right to access personal information we maintain, correct inaccurate or incomplete personal information, request deletion of personal information subject to legal and business limitations, receive portable copies of personal information in structured formats, and receive information about our data processing practices and policies.

We respond to rights requests according to the following timeframes:

European Union and European Economic Area requests: Within one month of receipt, with possible two-month extension for complex requests (GDPR Article 12(3))

Texas resident requests within 45 days of receipt, with possible 45-day extension communicated within the initial period (TDPSA Section 541.052(b)) including the right to opt out of targeted advertising, opt out of the sale of personal information to third parties, opt out of profiling activities that produce significant effects concerning the consumer, utilize universal opt-out mechanisms that we recognize and honor, and appeal our decisions regarding rights requests

Canadian user requests within 30 days unless circumstances require extension (PIPEDA)

Other jurisdictions: within 30 days unless applicable law specifies different timeframes.

Users may exercise privacy rights by submitting requests to support@resin8.ai with sufficient information to verify identity and specify the rights being exercised.

8. DATA RETENTION AND DELETION PRACTICES

We retain personal information for the minimum period necessary to fulfill the purposes for which it was collected, comply with legal obligations, resolve disputes, and enforce our agreements. Retention periods vary based on the type of information, applicable legal requirements, business needs, and user relationship status.

Account information is retained for the duration of the user relationship plus seven years to comply with business record requirements, potential legal claims, and regulatory obligations. Transaction records are maintained for seven years after transaction completion to satisfy tax, accounting, audit, and regulatory requirements. Communication records are retained for three years to support customer service, dispute resolution, and legal compliance needs.

Artificial intelligence training data is processed according to the following framework: (a) Personal data used for AI training is pseudonymized and retained for seven years maximum unless business necessity requires longer retention; (b) Data that has been anonymized through irreversible processes rendering re-identification impossible may

be retained indefinitely as it no longer constitutes personal data; and (c) Aggregated statistical data containing no individual identifiers may be retained indefinitely for analytics and research purposes. We implement technical measures including data minimization, access controls, and periodic review to ensure AI training datasets comply with applicable retention limitations.

Legal retention requirements may extend retention periods beyond standard practices when required by tax laws, regulatory obligations, litigation holds, government investigations, or other legal processes. We regularly review retention practices and delete personal information when retention is no longer necessary or legally required.

9. DATA SECURITY AND PROTECTION MEASURES

We implement comprehensive technical safeguards including encryption of personal information in transit using industry-standard protocols, encryption of personal information at rest using appropriate algorithms and key management, access controls and authentication systems limiting data access to authorized personnel, network security monitoring and intrusion detection systems, regular security assessments and vulnerability testing, and secure software development practices and code review procedures.

Organizational security measures encompass employee training on data protection and security practices, confidentiality agreements and security obligations for all personnel with data access, vendor security assessments and contractual security requirements, incident response procedures for data breaches and security events, regular policy reviews and security procedure updates, and data protection impact assessments for new processing activities.

Physical security controls protect facilities and systems through restricted access to data centers and office facilities housing personal information, environmental controls and monitoring systems for equipment protection, secure disposal procedures for hardware and storage media containing personal information, backup and disaster recovery procedures ensuring data availability and integrity, and visitor management and facility security protocols.

We maintain incident response procedures to promptly investigate security incidents affecting personal information, notify affected individuals and regulatory authorities as required by applicable law, implement remediation measures to address security vulnerabilities and prevent recurrence, provide regular updates on incident resolution

progress to affected parties, and conduct post-incident reviews to improve security practices and procedures.

10. THIRD-PARTY PROCESSORS AND SERVICE PROVIDERS

We engage third-party processors and service providers for cloud infrastructure and hosting services, payment processing and financial transaction handling, identity verification and fraud prevention services, customer support and communication platforms, analytics and business intelligence tools, marketing and advertising platforms, and cybersecurity and monitoring services.

All third-party processors must enter into data processing agreements containing appropriate privacy and security protections, implement technical and organizational measures meeting our security standards, process personal information only according to our documented instructions, notify us of data breaches and security incidents affecting our data, permit and cooperate with audits and assessments of their data processing practices, and maintain confidentiality regarding personal information processed on our behalf.

We conduct due diligence on third-party processors including security assessments, privacy policy reviews, compliance verification procedures, reference checks and reputation evaluation, and ongoing monitoring of processor performance and compliance. We maintain an updated list of active processors and subprocessors available through our Privacy Policy.

Users consent to our engagement of third-party processors for platform operations and service delivery. We provide reasonable notice of material changes to our processor relationships and maintain appropriate contractual protections for all third-party processing arrangements.

11. CROSS-BORDER DATA PROCESSING COMPLIANCE

Our international operations require processing personal information across multiple jurisdictions with varying data protection requirements. We maintain compliance frameworks addressing European Union General Data Protection Regulation requirements for EU resident data, Canadian Personal Information Protection and Electronic Documents Act obligations for Canadian data, Texas Data Privacy and Security Act compliance for Texas resident information, and other applicable jurisdictional requirements based on user location and data source.

Transfer mechanisms include Standard Contractual Clauses for EU data transfers, adequacy decisions where available for specific destinations, binding corporate rules for intra-company transfers, consent-based transfers where appropriate and legally sufficient, and supplementary measures including encryption, access controls, and impact assessments for restricted transfers.

We monitor international data protection developments including new adequacy decisions, updated standard contractual clauses, regulatory guidance on transfer mechanisms, court decisions affecting international transfers, and changes in third-country data protection laws. We adjust our compliance practices as necessary to maintain lawful transfer authority and protect personal information across borders.

12. BREACH NOTIFICATION AND INCIDENT RESPONSE

We maintain comprehensive incident response procedures to address data breaches and security incidents affecting personal information. Upon discovering a breach, we conduct immediate containment and assessment activities, investigate the scope and cause of the incident, implement remediation measures to prevent further unauthorized access or disclosure, and assess the risk to affected individuals and appropriate response measures.

Breach notification obligations vary by jurisdiction:

> European Union: We notify the competent supervisory authority within 72 hours of becoming aware of breaches likely to result in a risk to individual rights and freedoms (GDPR Article 33(1)). We notify affected individuals without undue delay when breaches are likely to result in a high risk to rights and freedoms (GDPR Article 34(1)).
>
> Texas: We notify the Texas Attorney General without unreasonable delay for breaches affecting 50 or more Texas residents (TDPSA Section 541.053(a)).
>
> Other jurisdictions: We comply with applicable breach notification timeframes and thresholds as required by law.

We maintain records of all data breaches including the facts relating to the breach, its effects, and remedial action taken. These records enable demonstration of compliance with notification obligations and support ongoing security improvement efforts.

Users will receive prompt notification of breaches affecting their personal information along with information about the nature of the breach, potential consequences, and measures being taken to address the incident and prevent recurrence.

13. DATA PROTECTION IMPACT ASSESSMENTS

We conduct data protection impact assessments for processing activities likely to result in high risk to individual rights and freedoms including new data processing technologies or systems, large-scale processing of sensitive personal information, systematic monitoring of publicly accessible areas, automated decision-making with significant effects, processing involving innovative technologies or novel applications, and cross-border transfers to countries without adequate data protection frameworks. Where a data protection impact assessment indicates that processing would result in high risk to individual rights and freedoms absent mitigating measures, and where we cannot identify sufficient safeguards to reduce such risk, we consult with the competent supervisory authority prior to commencing processing as required by GDPR Article 36.

Assessment procedures include identifying and describing processing activities and their purposes, evaluating the necessity and proportionality of processing activities, assessing risks to individual rights and freedoms, identifying measures to address risks and demonstrate compliance, consulting with stakeholders including data protection officers and affected individuals where appropriate, and documenting assessment results and mitigation measures.

We regularly review and update impact assessments to reflect changes in processing activities, technological developments, legal requirements, risk factors, or stakeholder concerns. Consultation with competent supervisory authorities occurs when assessments indicate high residual risks that cannot be adequately mitigated.

14. CONTACT INFORMATION AND SUPERVISORY AUTHORITY DETAILS

Our primary privacy contact is available at support@resin8.ai for all data protection inquiries, rights requests, complaints, and general privacy matters. Our legal team handles complex privacy questions, regulatory inquiries, and formal legal correspondence. Written correspondence may be sent to our business address at 1209 Orange Street, Wilmington, New Castle County, Delaware 19801.

Users may file complaints with appropriate supervisory authorities if not satisfied with our response to privacy concerns. European Union users may contact their national data protection authority or the lead supervisory authority in Ireland where applicable. Canadian users may file complaints with the Privacy Commissioner of Canada at https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/. Texas residents may contact the Texas Attorney General's Office at

https://www.texasattorneygeneral.gov/consumer-protection/file-consumer-complaint or (800) 621-0508.

We maintain cooperative relationships with supervisory authorities and respond promptly to official inquiries, investigation requests, and enforcement proceedings. We participate in regulatory consultations and industry initiatives to promote effective data protection practices and compliance frameworks.

15. MODIFICATIONS AND EFFECTIVE DATE

We may update this Data Processing Agreement to reflect changes in applicable law, new processing activities, updated security measures, technological developments, or regulatory guidance from competent authorities. Material changes affecting data processing practices will be communicated through prominent notice on our platform, direct notification to account holders, and other appropriate means based on the significance of changes.

Notice periods for Data Processing Agreement changes include thirty days advance notice for material changes affecting processing purposes or user rights, fourteen days notice for changes required by legal or regulatory developments, and immediate notice for emergency changes necessary to protect data security or comply with urgent legal requirements.

This Agreement becomes effective on the date listed above and supersedes all prior data processing agreements and privacy notices. Previous versions remain available upon request for users who need to reference historical privacy practices for legal or business purposes.

By using our platform, you acknowledge that you have read and understood this Data Processing Agreement and consent to the data processing practices described herein in accordance with applicable law.