
Ai Inventory Pro Platform Privacy Agreement and Notice

Version 1.0 | October 16, 2026 | Pre-launch notice and proposed customer terms

This notice covers aiinventorypro.com and the WindFire ERP platform, platform portal, customer workspaces, applications, support, and connected features being developed under the planned Ai Inventory Pro name ("WindFire", "we", or "us"). The project is pre-launch, has no customers yet, and Ai Inventory Pro is not yet an established business entity. Edward Gilbert is the project contact responsible for privacy questions during this pre-launch period. The future contracting entity will be identified before customer agreements are accepted. It explains current website and pre-launch privacy practices and the rules intended to govern future customer workspaces. References to customers, bank feeds, and production integrations describe planned services and obligations; they do not represent that customer processing has started or that every required control has been implemented. Production processing must meet the applicable requirements before it begins. It does not cover an unrelated service merely because that service uses an aiinventorypro.com subdomain. Edward Gilbert is the Privacy Officer and can be contacted at info@aiinventorypro.com.

1. Your data and our responsibilities

As between WindFire and its business customer, the customer retains ownership of its workspace records, files, and other Customer Data. Individuals retain their legal rights in personal information about them. Data ownership does not remove those rights or excuse either party from applicable privacy law.

For information entered into a customer workspace, the customer ordinarily determines the purposes of processing and acts as the controller or responsible organization. WindFire acts as its processor or service provider under documented instructions. WindFire separately determines the purposes of processing its own website inquiries, account administration, subscription billing, security, and legal records. The role depends on the particular processing, not just the label in a contract.

This notice supplements the Customer Agreement, module schedules, and security policies. It does not authorize an optional integration, constitute an individual's consent to every possible use, or retroactively amend a signed contract. Mandatory privacy rights and obligations prevail over inconsistent contract terms. No arbitration, choice-of-law, liability, or customer-ownership provision waives rights that applicable law does not allow to be waived, including the right to contact a regulator.

2. Information, sources, purposes, and recipients

The categories below describe information the platform is designed to handle. Actual collection depends on the features a customer selects and the information provided. The customer must give affected people any additional workplace or collection-specific notice that its use requires. We do not require every category from every user.

Account and contact identifiers: names, work email addresses, organization, role, account identifiers, and contact details come from the individual, the customer's administrator, or an authorized identity provider. We use them for account creation, authentication, permissions, communications, and support. Necessary hosting, authentication, and email providers may process the relevant information; authorized customer users see information permitted by their roles. Retention follows the account and support criteria in section 8.

Commercial and billing information: subscription selections, invoices, billing contact information, payment status, and transaction references come from customers, their use of the service, and payment processors. We use them to supply and bill for the service and maintain financial records. Payment processors and necessary hosting providers receive the information required for those tasks. Full payment credentials entered in a processor's hosted interface are handled under that processor's notice. Retention follows the statutory business-record criteria in section 8.

Customer business records: inventory, sales and purchase records, supplier and customer contacts, accounting, tax, payroll, employment, quality, and uploaded documents come from customer users and authorized imports or integrations. They are processed to perform the selected ERP functions and preserve business-record integrity. Necessary hosting and backup providers process stored records; additional providers receive relevant records only for an enabled function. Retention follows customer instructions and the business-record and workspace-closure criteria in section 8.

Bank information: account identifiers, account information made available with permission, and transactions come through the bank-connectivity provider selected during connection. We use the authorized information to import transactions, match records, and support reconciliation. The selected bank-connectivity provider, the financial institution, and necessary hosting providers participate in this processing. Raw integration payloads, connection credentials, and imported accounting records have distinct retention rules in section 8.

Technical and security information: IP address, browser and device information, sign-in and session events, audit events, service usage, and error information come from devices and operation of the service. We use them to provide the site, authenticate access, prevent abuse, investigate faults and incidents, and understand aggregate service performance. Necessary hosting, infrastructure, and security providers may process them. Retention follows the log and security-evidence criteria in section 8.

Support and communications: requests, correspondence, attachments, support grants, and the resulting access records come from the requester, authorized staff, and the service. We use them to answer the request and document authorized assistance. Necessary hosting and communications providers process them. Please do not include passwords, bank sign-in credentials, or unnecessary sensitive records. Retention follows the support and audit criteria in section 8.

Workforce, location, and images: customer-enabled Tracker and workforce functions may process work time, activity, location, photographs, and employment information. The customer must identify the specific collection, purpose, and consequences before use and obtain any required consent. Device permissions and feature controls affect collection. These records are used for the customer's selected workforce function and may be visible to its authorized managers and necessary infrastructure providers. Retention follows the applicable employment-record schedule; precise location and images must not be kept merely because other payroll records require longer retention.

Sensitive personal information may occur within these categories, including financial account details, tax or government identifiers, login credentials, precise location, and sensitive employment information. We restrict its use to the requested service, permitted security purposes, customer instructions, and applicable legal obligations. Do not upload sensitive information that is unnecessary for the chosen function. A photograph is not by itself authorization to create a biometric identifier or perform facial recognition.

3. Limited use, no sale, and customer choices

WindFire does not sell Customer Data or authorize its use for advertising or data brokerage. We do not authorize providers to use customer business records to train general-purpose AI models. Necessary processing to deliver the service is distinct from a sale or advertising disclosure. We do not use customer business records for cross-context behavioral advertising or targeted advertising.

We limit processing to the purposes described here and the customer's documented instructions. Optional functions must be selected or enabled; declining an optional function does not authorize unrelated processing. Where consent is required, it must identify the relevant information, purposes, recipients, and material consequences. A materially different purpose requires a new notice and any legally required consent before that processing begins. Consent cannot legitimize an otherwise prohibited use.

We may use aggregate or de-identified operational statistics to measure availability and performance. Information treated as de-identified must not reasonably identify a person, and we must maintain safeguards against re-identification and require equivalent restrictions from permitted recipients. Pseudonymous account identifiers alone are not anonymous data.

4. Platform personnel and support access

WindFire personnel may access customer business records for ordinary support only with the customer's express, recorded permission through a time-limited workspace support grant. The grant specifies scope and duration and may be revoked. An electronic grant is recorded written authorization. Customer users remain subject to the customer's role and access controls.

The existing Customer Agreement allows narrow operational access strictly necessary to secure, back up, restore, or operate infrastructure, and access required by law. These exceptions do not authorize routine browsing of business records. Such access must be purpose-limited, restricted to authorized personnel, logged, and reviewed. Automated hosting and backup

processing is necessary to operate the service and is not a representation that the platform is technically incapable of processing stored data.

5. Necessary providers and optional integrations

Only providers needed to operate the service or supply a customer-enabled feature may process relevant information. Hosting and backup providers support infrastructure; payment processors handle billing; communications providers deliver requested messages; bank-connectivity providers support chosen bank feeds; and optional AI, mapping, shipping, tax, cloud-storage, and other integrations process the information needed for their selected functions. Permission to use one integration does not authorize another.

Processors acting for WindFire must be subject to written instructions, confidentiality, security, limited-purpose use, retention and deletion, incident reporting, and assistance obligations appropriate to their role and applicable law. We remain responsible for our processor obligations. A provider acting independently, such as a bank or a payment provider for its own legal obligations, also has responsibilities described in its own notice. Its independent role does not excuse WindFire's obligations.

Customers and individuals may request the applicable provider identities, processing purposes, countries, and privacy information from the Privacy Officer before enabling a feature. Customer-controlled connections may use a provider selected by the customer. Disclosure to a provider is limited to the information needed for that connection; a provider's general terms do not grant WindFire permission for unrelated reuse.

We may disclose information when legally required, limited to the lawful request and with notice to the customer when permitted. We do not disclose customer business records to advertisers or data brokers. A business reorganization or transfer would remain subject to applicable confidentiality, notice, consent, and purpose restrictions; it would not authorize unrestricted sale or reuse of customer records.

6. Bank feeds and payments

A customer may choose Stripe Financial Connections or an available Plaid connection. The provider presents its own connection and consent process. We use authorized bank data to import, review, match, and reconcile records within the customer workspace. This bank-feed authorization does not authorize WindFire to move money, make a credit decision, or automatically post imported transactions to the ledger. Payment processing is a separate function and authorization.

WindFire does not receive bank sign-in credentials through the bank-feed feature. Connecting a bank does not authorize sending its transaction data to AI providers, advertisers, or unrelated services. Disconnecting ends future access through that connection, subject to processing already underway and the provider's revocation mechanism. Previously imported accounting records are handled under the applicable retention requirements. A customer can request deletion separately; disconnecting does not itself erase provider-held records.

Stripe's own privacy information is available at <https://stripe.com/privacy> and Plaid's at <https://plaid.com/legal/#end-user-privacy-policy>. Stripe Financial Connections currently supports US bank accounts. Canadian bank-account syncing is not yet available. Availability depends on the particular institution and account; this notice does not promise every bank is supported.

7. AI, automated decisions, cookies, and communications

Optional AI functions may transmit the relevant prompt, selected context, and associated content to the configured model provider to produce a response. A user must have authority to include personal information in a request. Customer authorization to use AI is not permission for the provider to train a general-purpose model on customer business records. Customers must review outputs before making consequential decisions and obtain any additional notices, assessments, or consents required for their use.

If processing subject to applicable law involves a solely automated decision or profiling with legal or similarly significant effects, the responsible organization must give the required notice and provide applicable access, explanation, correction, objection, opt-out, or human-review rights. A general agreement or an AI disclaimer does not replace those safeguards. Contact the Privacy Officer about processing WindFire controls or the customer's administrator about customer decisions; we will assist

with routing a request.

On the public website, the product assistant sends your question and up to six recent conversation messages to the OpenAI API. Its conversation history remains in the current browser page and clears on reload; the website does not save those assistant transcripts in its own database. Requests use `store:false`, which does not remove the provider's applicable security and abuse-monitoring retention. OpenAI's notice is at <https://openai.com/policies/privacy-policy/>. The public assistant has product information, not access to tenant records.

If you choose Talk to a person, your name, email, optional company, messages, replies, and last six assistant questions are sent to the WindFire Sales desk for follow-up. Messages are machine-translated. Website inquiries are delivered to info@aiinventorypro.com and routed to the domain administrator's mailbox; deletion is handled through the Privacy Officer. The language preference is stored locally in your browser. The public site uses a short-lived security cookie and hashed network-address rate-limit counters for up to two days; hosting logs may contain network addresses, pages, timestamps, and browser information. The current public website does not use advertising trackers or third-party analytics.

The service uses technical storage and session mechanisms needed for authentication, security, and chosen settings. A nonessential analytics, advertising, location, or profiling function requires the notices and choices applicable to that function before it is enabled. Browser controls can remove or restrict cookies, although disabling necessary session storage can prevent sign-in. Our prohibition on sale and advertising use of customer business records applies regardless of a browser signal. We do not treat a missing opt-out signal as consent. Where a legally recognized opt-out signal applies to processing we control, it must be honored; contact us if a choice appears not to work.

Service, security, billing, and requested support messages are used to administer the service. Promotional communications require the permission or other lawful basis required in the recipient's jurisdiction and an available unsubscribe method. Withdrawing marketing permission does not stop necessary service notices.

8. Retention and deletion

We retain information only while necessary for the disclosed purpose, customer instructions, and applicable legal or record-preservation obligations. The following criteria and maximum periods derive from WF-SEC-004. They are policy requirements, not permission to retain every record for the longest period. A shorter legal deadline or valid deletion request takes priority unless a lawful exception applies.

Account administration and ordinary support: keep while the account or request is active and while necessary to complete closure, resolve a dispute, or meet an identified legal obligation. After closure, the workspace export and deletion limit below applies to workspace copies. Subscription financial records and minimal proof of requests follow their separate schedules. Inquiry information must be deleted when the inquiry and any permitted follow-up purpose end, unless it becomes a customer record or a documented obligation requires retention.

Closed workspaces: up to 90 days after termination for authorized export and closure, then deletion unless specific lawful retention is documented. A valid erasure request or shorter applicable deadline can require earlier action.

Accounting, tax, payroll, employment, and transaction records: the period depends on the record type, jurisdiction, filing period, statutory requirement, and any valid dispute or preservation obligation. The customer and WindFire must identify that requirement in the retention register rather than assume a universal period. Access during required retention is limited to the retained purpose. Precise location, photographs, and raw integration content must be assessed separately from derived payroll or accounting records.

Transient integration payloads: delete within 30 days after successful processing unless an identified necessary record purpose requires retention. Temporary exports and processing files: delete within 7 days of creation. Customer-downloaded copies are controlled by the customer.

Integration credentials: revoke access promptly when authorization ends or compromise is identified, and remove active credentials when revocation completes. Do not preserve usable credentials merely for archival purposes.

Security event logs: 90 days. Access-review and ordinary security audit evidence: 12 months. Legally required incident, privacy-request, or litigation records may require a different documented period; routine log expiry must not erase them

prematurely.

Recovery backups: rolling expiry no longer than 35 days unless a separately documented lawful recovery or preservation requirement applies. Deleted active data may remain in isolated backups until expiry. Restoring a backup requires reapplying deletion and restriction instructions before ordinary use resumes.

A legal hold must specify its basis, scope, access restrictions, and review or release condition. When the reason ends, ordinary disposal resumes. We explain any permitted refusal or partial retention in response to a request and seek provider deletion or confirmation where we are responsible for their processing. Independent providers may retain information under their own lawful obligations.

9. United States hosting and Canadian information

WindFire customer data is hosted in the United States under the service's stated hosting arrangement. This includes Canadian customer data. Stripe Financial Connections bank data must be stored only in the United States. An integration or customer-directed export must not silently override that restriction. Provider processing locations and independent-provider obligations must be assessed for each enabled service.

Information processed outside Canada may be subject to foreign laws and lawful access by courts, law-enforcement, and national-security authorities. Contracts cannot eliminate that possibility. Contact Edward Gilbert at info@aiinventorypro.com for written information about providers, countries, purposes, safeguards, and transfer practices before using a connection. The same contact handles Alberta questions concerning service providers outside Canada.

Transfers remain subject to applicable legal safeguards. Where Quebec law applies, required privacy impact assessments and written safeguards must be completed before the relevant transfer outside Quebec or covered system project proceeds. Customer instructions do not substitute for an assessment required of WindFire, and customer consent does not remove mandatory safeguards. Canadian information is not represented as remaining in Canada.

10. Exercising privacy rights

Depending on the law and our role, you may request confirmation of processing; access to your information; information about sources, purposes, uses, and recipients; correction; deletion; a portable copy; withdrawal of consent; restriction or objection; and applicable opt-outs from sale, targeted advertising, or qualifying profiling. Where law provides a right to a list of specific third parties, to information about automated decisions, or to human review, you may request it through the same channels. Quebec rights may also include cessation of dissemination or de-indexing when the legal conditions are met.

Email info@aiinventorypro.com with the subject Privacy Request, or use your workspace's Support page. Tell us your relationship to the service, the request, and a safe way to reply. You do not need to create an account or purchase service to make a request. A request need not use our preferred subject line to be valid. Do not send passwords, complete bank numbers, or government identification in an ordinary email; we will arrange proportionate verification if needed.

If the information is controlled by your employer or another customer, you may contact its administrator directly. If you contact us, we will identify the responsible organization and assist with the request as required; a referral does not waive any obligation we have independently. We do not disclose another person's information or override a customer's lawful recordkeeping requirements merely because someone requests it.

An authorized representative may submit a request with evidence of authority. Where lawful and necessary, we may verify the individual's identity or confirmation of the agent's authority. We use information supplied for verification only for verification, security, and required request records. Opt-out requests do not require unnecessary identity verification.

11. Response times, appeals, and complaints

Our operating target is a substantive response within 30 calendar days after receipt, with earlier action where law requires it. We acknowledge receipt promptly and seek any necessary clarification or verification without avoidable delay. We apply the deadline, extension limits, and notice requirements of the governing law. An extension is used only when legally available; the requester receives its reason and revised deadline within the original deadline. Acknowledgment alone is not completion.

If we refuse all or part of a request, we explain the reason and applicable review or complaint options unless disclosure is legally prohibited. You may appeal or challenge our response by emailing the same address with Privacy Appeal and the request reference. We aim to give a reasoned written appeal decision within 30 days and always within the applicable legal period. You may appeal without using that subject line. If an appeal is denied, we provide the relevant regulator complaint route where required.

Requests are ordinarily free. Any lawful charge or refusal based on a manifestly unfounded, excessive, or otherwise exempt request must be explained under the applicable law. We do not discriminate or retaliate for exercising privacy rights. A requested deletion or withdrawal may make the affected optional function unavailable; we explain that consequence rather than impose an unrelated penalty.

You may contact a regulator without first completing our internal process where law permits. US residents may contact their state attorney general or privacy regulator; California residents may use <https://cppa.ca.gov/complaints/>. Canadian residents may contact the Office of the Privacy Commissioner of Canada at <https://www.priv.gc.ca/en/report-a-concern/>, or the applicable provincial regulator: Quebec at <https://www.cai.gouv.qc.ca/>, Alberta at <https://oipc.ab.ca/>, and British Columbia at <https://www.oipc.bc.ca/>.

12. California and other US state notices

Sections 2, 5, and 8 identify information categories, sources, purposes, recipient categories, and retention criteria. The categories may include identifiers; customer-record information; commercial information; internet or network activity; professional or employment information; geolocation; visual information; and sensitive information described in section 2. Protected-characteristic information may be present in customer-supplied employment records where relevant and lawful. Customer-supplied records and configured reports may contain inferences; their use follows the same purpose and access restrictions.

Where California law applies, residents may request the categories and specific pieces of information collected about them, sources, purposes, disclosure information, correction, deletion, and applicable limits on sensitive-information use and sale or sharing. Requests and authorized-agent requests follow sections 10 and 11. WindFire does not authorize sale or cross-context behavioral advertising use of customer business records, including those of people under 16. Necessary processor disclosures must meet the applicable service-provider requirements; calling a recipient a processor alone is insufficient.

Other state rights depend on the particular law, processing, and any lawful exemption. We accept requests through the same channels, including appeals and applicable rights concerning recipients, portability, sensitive information, and qualifying profiling. This notice does not claim every statute applies to every record, and a business-to-business relationship does not automatically remove all privacy duties.

13. Canadian consent, access, and accountability

We apply the privacy law relevant to the organization and activity, which may include PIPEDA and the private-sector laws of Quebec, Alberta, or British Columbia. We identify purposes and seek meaningful consent where required, with separate choices for processing unnecessary to supply the requested service. You can withdraw consent by contacting the Privacy Officer or using the relevant connection control, subject to lawful restrictions and reasonable notice. We explain consequences and any continuing lawful retention.

You may seek access, correction, information about uses and disclosures, and other applicable rights through sections 10 and 11. PIPEDA access requests generally require a response within 30 days; an extension requires a permitted reason and timely notice. Provincial requirements are applied where they govern. For Quebec portable-data requests, applicable computerized information supplied by the person is provided in a structured, commonly used technological format, subject to statutory limits.

The Privacy Officer oversees requests, complaints, provider accountability, retention, incident handling, and review of privacy practices. Internal access is restricted by role and need. Complaints are investigated and findings and corrective actions documented. Information about these practices and accessible formats of this notice may be requested from the Privacy Officer.

14. Security and incidents

Our security program requires appropriate administrative, technical, and physical safeguards proportionate to the information and risk, including tenant separation, authorized access, secure transmission, protected credentials, recovery controls, and access records. No system is completely secure. A policy does not represent a certification or eliminate the need to verify individual controls.

We investigate suspected incidents, contain and remediate confirmed issues, preserve necessary evidence, and notify customers, affected individuals, and authorities as required by our role, applicable law, and contract. We do not delegate away notification duties that law places directly on WindFire. Where acting for a customer, we provide timely information and assistance so the customer can meet its duties. Required incident records are maintained separately from ordinary log disposal.

15. Children, regulated uses, and workplace monitoring

The platform is intended for business use and is not directed to children. Customer administrators must assess any information about minors and obtain lawful parental or other authorization where required. If we learn that information has been collected unlawfully, we will investigate and take the required corrective action.

A general ERP subscription does not itself establish compliance for health-care records, biometric identification, consumer health-data processing, credit reporting, financial advice, or other separately regulated activities. Such a use requires its own legal basis, notices, agreements, and controls before processing. Employment, payroll, location, photography, and monitoring likewise require customer-specific legal review and notices where applicable. Do not enable prohibited or unsupported processing on the assumption that this general notice authorizes it.

16. Contact, availability, and changes

Privacy Officer: Edward Gilbert, Ai Inventory Pro / WindFire ERP. Email: info@aiinventorypro.com. Existing customers may also use the workspace Support page. Ask this contact for an accessible copy, provider and transfer details, a privacy request, or a complaint. No one should send confidential records through an unsecured public form.

This pre-launch notice is dated October 16, 2026. We will identify the effective date and legal operator of a customer-service notice before production launch, retain prior published versions, and give notice of material changes as required. New uses require any legally required choice or consent before they begin. Publishing a revised notice does not retroactively authorize a new use. The proposed customer terms below are not a signed agreement and must be completed and accepted before they become contractual. This notice does not change an existing signed agreement until its applicable amendment process is completed.

Appendix A. Customer data-processing terms for acceptance

Status: proposed contractual supplement. These terms become contractual only through the applicable provider and customer acceptance process. Mandatory legal duties apply independently of acceptance. The provider must be the confirmed legal operator of WindFire ERP, not an entity that has not yet been established. The customer is the business identified in the Customer Agreement. The proposed Ai Inventory Pro business name does not itself establish a legal entity or create a signature. These terms must not be accepted until the provider identity is completed.

Instructions and scope: WindFire processes personal information in Customer Data only on the customer's documented instructions to supply the selected services, during the subscription and limited closure/retention period, or as law requires. The subject matter is hosted ERP processing, support, security, recovery, and authorized integrations. Processing may include collection, storage, organization, retrieval, calculation, transmission, export, correction, and lawful deletion. Data subjects include customer personnel, customers, suppliers, contractors, and other people whose information the customer lawfully provides. Categories are those in section 2 and the applicable module configuration. Customer instructions cannot authorize unlawful processing; WindFire will inform the customer if an instruction appears to violate applicable privacy law and suspend the affected instruction while it is resolved.

Purpose limits: WindFire will not sell or share Customer Data for cross-context behavioral advertising, retain/use/disclose it outside the specified business purposes or direct business relationship except as law permits, or combine personal information from unrelated customers or independent sources except as expressly permitted by applicable law and the documented instructions. WindFire will provide the level of privacy protection required of its processing role and notify the customer if it can no longer meet those obligations. The customer may take reasonable steps to verify compliance and stop and remediate unauthorized use.

People and safeguards: personnel with access must be bound by confidentiality, trained for their duties, and given only necessary access. Support access follows section 4. WindFire will maintain safeguards appropriate to the nature and risk of the processing, review them, and provide relevant information needed to assess those safeguards without disclosing other customers' records, credentials, or security-sensitive exploit details.

Subprocessors: the customer authorizes necessary providers and customer-selected optional providers within the scope of this agreement. WindFire will identify its subprocessors and their functions and give advance notice of additions or replacements where required by law or contract, allowing a reasonable opportunity to object on privacy grounds. The parties will resolve an objection through an alternative arrangement or discontinuation of the affected processing where necessary. WindFire will bind its subprocessors in writing to applicable equivalent data-protection obligations and remain responsible for its own obligations. Independent providers selected by the customer are identified by their role and are not misrepresented as WindFire's subprocessors.

Assistance: taking account of the nature of processing and information available, WindFire will assist with individual rights requests, security incidents, privacy/risk assessments, regulator inquiries, and lawful customer compliance duties. Direct requests concerning customer-controlled data will be communicated to the customer promptly unless law prohibits it; WindFire will not independently dispose of legally required business records without a lawful basis. Assistance will preserve record integrity and other persons' rights.

Incidents: WindFire will notify the customer of a personal-data incident without undue delay and within the applicable legal or contractual deadline, provide available information needed for assessment and response, and update it as the investigation develops. The parties will coordinate notices without restricting any nondelegable duty. Neither party must wait for a complete forensic report where law requires earlier notice.

Return, deletion, and retention: on termination or the customer's lawful instruction, WindFire will return or delete personal information and require applicable subprocessor disposal, except for specific legally required retention. Restricted backups expire under the approved schedule and deletion instructions are reapplied after restoration. Retention exceptions are documented, restricted to their lawful purpose, and reviewed. Deletion completion is reported only after verification; an unfinished provider or backup action is identified as pending.

Evidence and audit: WindFire will provide information reasonably necessary to demonstrate compliance with these terms and cooperate with reasonable assessments or audits required by applicable law, using proportionate confidentiality and security arrangements. Relevant independent reports may satisfy a request where appropriate, but cannot eliminate a legally required audit or conceal a material deficiency. The customer must not receive another tenant's information.

International processing: United States hosting and provider transfers follow section 9 and applicable transfer restrictions. Required assessments, safeguards, notices, and agreements must precede the affected processing. A change in hosting or provider location requires the applicable review and customer notice; it cannot silently defeat a bank-data storage restriction.

Order of priority: mandatory privacy law prevails. Once accepted, these specific data-processing terms govern over conflicting general agreement terms for their subject matter. They do not grant a waiver of individual rights, remove WindFire's responsibility for its own providers, or authorize general-purpose model training on Customer Data. Existing signed versions remain unchanged until valid amendment or replacement.