

Privacy Policy – jenX Global Partners

Effective Date: October 24, 2025

Last Updated: October 24, 2025

jenX Global Partners (operating under the trade name of jenX Global Partners LLC, registration anticipated in 2026)

8407 Bandera Rd, Suite 103-271

San Antonio, TX 78250, USA

Phone: +1 (210) 595-0415

Email: privacy@jenx.ai

1) General Information & Scope

1.1 Definitions

For purposes of this Privacy Policy, the following terms shall have the meanings set forth below:

“Personal Data” (or “Personal Information”) means any information relating to an identified or identifiable natural person. This includes, without limitation, names, email addresses, identification numbers, online identifiers, employment details, location data, IP addresses, and any other data that can directly or indirectly identify an individual.

“Processing” means any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, use, disclosure, transmission, dissemination, combination, restriction, erasure, or destruction.

“Data Controller” (or “Controller”) refers to the natural or legal person that determines the purposes and means of the Processing of Personal Data. For most activities described herein, jenX Global Partners acts as the Data Controller.

“Data Processor” (or “Processor”) refers to any natural or legal person that processes Personal Data on behalf of the Controller. For certain services, jenX’s third-party service providers or Virtual Assistant (VA) Staff may act as Processors under jenX’s direction and subject to appropriate data-processing agreements.

“Data Subject” refers to the individual to whom the Personal Data relates.

“Applicable Data Protection Laws” means all laws and regulations governing privacy and data protection in the jurisdictions in which jenX operates, including but not limited to the GDPR, UK GDPR, CCPA/CPRA, PIPEDA, the Australian Privacy Act, and the Philippine Data Privacy Act.

“Cookies” means small text files or similar technologies that are stored on a user’s device to enable website functionality, analytics, personalization, or advertising.

“Anonymization” refers to the process by which Personal Data is altered so that it can no longer be attributed to an identifiable individual, whether directly or indirectly.

“Pseudonymization” means the processing of Personal Data in such a manner that it can no longer be attributed to a specific individual without the use of additional information kept separately and protected by technical and organizational safeguards.

1.2 Data Controller & Contact Information

The entity responsible for determining the purposes and means of processing your Personal Data is:

jenX Global Partners

Attn: Data Protection Officer – Jennie Largent

8407 Bandera Rd, Suite 103-271

San Antonio, TX 78250, USA

Email: privacy@jenx.ai

This Privacy Policy forms an integral part of jenX Global Partners’ Terms of Service and should be read together with those Terms. jenX Global Partners serves as the Data Controller for all processing activities described in this Policy. Questions, concerns, or requests to exercise privacy rights should be directed to the email address above.

If jenX expands its operations to the European Union or United Kingdom, it will appoint an authorized representative in accordance with Article 27 of the GDPR and update this Privacy Policy to reflect that appointment.

1.3 Global Application and Legal Basis

This Privacy Policy applies globally to all users, clients, contractors, and website visitors. jenX Global Partners complies with applicable privacy and data-protection laws in the jurisdictions where it operates or from which it collects data, including the GDPR, UK GDPR, CCPA/CPRA, PIPEDA, the Australian Privacy Act, and the Philippine Data Privacy Act. Where local law provides additional protections or rights, those provisions apply in addition to this Policy.

jenX processes Personal Data on one or more of the following legal bases, as permitted by Applicable Data Protection Laws:

- Performance of a contract or pre-contractual obligations;

- Compliance with a legal obligation;
 - Legitimate business interests pursued by jenX or a third party;
 - Consent of the Data Subject, where required by law; and
 - Protection of vital interests or public interest.
-

1.4 Updates to this Privacy Policy

jenX may update this Privacy Policy periodically to reflect operational, legal, or regulatory changes. The “Effective Date” at the top of this Policy indicates the most recent revision. Material changes will be communicated through our website or by direct notice where required by law. Your continued use of jenX services after such updates constitutes acceptance of the revised Policy.

2) Information We Collect

2.1 Categories of Personal Data Collected

jenX Global Partners (“jenX”) collects and processes Personal Data as necessary to operate, improve, and provide its Services. The categories of Personal Data collected include, but are not limited to:

A. Identifiers

- Full name, business name, job title, email address, phone number, and mailing address.
- Account credentials and authentication information for client portals or communication systems.

B. Commercial Information

- Billing details, service history, purchase records, invoices, and related transaction information.
- Payment data is collected through secure, third-party payment processors; jenX does not store full credit-card numbers or banking credentials.

C. Internet, Device, and Technical Information

- IP address, browser type, operating system, device identifiers, geographic location (approximate), access times, and referring website addresses.
- Log data relating to system performance, security, and usage trends.
- Data collected through cookies, consent banners, analytics tools, and similar technologies (see Section 2.3).

D. Professional, Employment, and Business Information

- Business affiliations, job function, company name, and related contact information.
- For clients engaging in VA or staffing services, this may include organizational details, project descriptions, and business processes necessary to perform the Services.
- For Virtual Assistants, contractors, or job candidates, this may include employment history, résumés, background information, and identification documents (e.g., driver’s license, government ID, or proof of residence) solely for verification, compliance, or payroll onboarding purposes.

- For individuals who participate in the jenX Partner or Connector Program, jenX may collect limited business and payment information (such as name, email address, bank account information, or tax ID numbers) for verification, compensation, and compliance purposes. All such information is processed in accordance with this Privacy Policy and applicable data-protection laws.

E. Communications and Interactions

- Records of correspondence, support requests, meeting notes, service feedback, chat transcripts, and email communications.

F. Marketing and Behavioral Data

- Data regarding website interactions, ad performance, email engagement, campaign participation, and referral or affiliate activities.
- Audience segmentation data, marketing preferences, cookie-consent status, and opt-in logs.

G. Sensitive or Special Categories of Data (if applicable)

- jenX does not intentionally collect sensitive personal data (such as racial or ethnic origin, health data, political opinions, or religious beliefs).
- If such data is provided by a client in connection with a project, jenX will process it only under strict confidentiality and in accordance with applicable law.

2.2 Sources of Personal Data

jenX obtains Personal Data from the following sources:

- Directly from you – when you register, complete a form, make a purchase, subscribe, apply for a position, or otherwise interact with us.
- Automatically – through cookies, analytics, and tracking tools that record activity on our websites and digital platforms after you provide consent via the cookie banner.
- From third parties – including marketing networks, payment processors, background-screening services, and communication platforms used to deliver the Services.
- From VA Staff activities – when Virtual Assistants or contractors perform services under your direction, jenX may collect operational data and access logs as part of oversight, compliance, or quality monitoring.

2.3 Cookies, Analytics, and Tracking Technologies

jenX uses cookies and similar technologies to enable core site functionality, improve user experience, analyze performance, and deliver personalized marketing.

Types of cookies used:

- Essential Cookies – required for website operation, authentication, and security.
- Performance and Analytics Cookies – used to measure website usage, identify trends, and improve

content (e.g., Google Analytics, server logs).

- Advertising Cookies – used for retargeting or measuring ad performance on platforms such as Meta, LinkedIn, and Google Ads.
- Functional Cookies – remembering preferences, forms, and chat sessions.

All users are presented with a cookie consent banner on first visit, allowing them to Accept all or Accept essential cookies. Non-essential cookies are blocked until consent is granted. Consent records are maintained in accordance with applicable data-protection laws.

You may control or delete cookies through your browser settings and may change or withdraw consent at any time via the Cookie Preferences link in the website footer. For more details, see Section 7 (Individual Rights and Choices).

2.4 Data of Minors

jenX's Services are intended for business users and are not directed toward children. jenX does not knowingly collect or process Personal Data from individuals under:

- 16 years of age in the European Union or United Kingdom;
- 13 years of age in the United States; or
- any higher minimum age required by applicable law.

If jenX becomes aware that it has inadvertently collected Personal Data from a minor without appropriate consent, it will take prompt steps to delete such data.

3) How We Use Personal Data

jenX Global Partners ("jenX") processes Personal Data only as necessary to provide, maintain, and improve its Services, fulfill contractual and legal obligations, and conduct legitimate business operations.

3.1 Primary Purposes of Processing

jenX uses Personal Data for the following purposes:

- Service Delivery and Operations – to provide and manage Services, including onboarding, project execution, account setup, client communications, and technical support.
- Billing and Administration – to process payments, issue invoices, manage subscriptions, and prevent fraud or unauthorized transactions.
- Recruitment and Staffing – to evaluate and onboard Virtual Assistants, contractors, and staff for client assignments, including background verification and compliance checks.
- Marketing, Communications, and Relationship Management – to send newsletters, service updates, promotional materials, or other information consistent with your preferences and applicable law.
- Analytics and Improvement – to analyze performance, monitor usage patterns, and enhance website functionality, security, and service quality.

- Legal and Regulatory Compliance – to comply with applicable laws, regulations, tax requirements, export controls, and record-keeping obligations.
- Security and Risk Management – to detect, investigate, and mitigate fraud, unauthorized access, or other harmful activity.
- Dispute Resolution and Enforcement – to enforce contracts, collect debts, or defend legal claims.

jenX limits the collection and processing of Personal Data to what is proportionate and necessary for the purposes described in this Privacy Policy, consistent with the principle of data minimization under applicable privacy and data-protection laws. Data is retained, accessed, and used only to the extent required to fulfill lawful business purposes or compliance obligations.

3.2 Lawful Bases for Processing (GDPR / UK GDPR)

Where the EU or UK General Data Protection Regulation applies, jenX relies on one or more of the following lawful bases to process Personal Data:

- Contractual Necessity – processing is required to perform a contract with you or to take steps at your request before entering into a contract.
- Legitimate Interests – processing is necessary for our legitimate business purposes, including improving services, securing systems, and maintaining relationships, provided these interests are not overridden by your rights and freedoms.
- Consent – where required (e.g., marketing communications, analytics, or cookie use), jenX processes data only after obtaining your freely given, informed consent, which may be withdrawn at any time.
- Legal Obligation – processing is necessary to comply with applicable laws or lawful requests by public authorities.
- Vital Interests – in rare circumstances, processing may occur to protect an individual’s life, health, or safety.

3.3 Data Retention

jenX retains Personal Data only for as long as necessary to fulfill the purposes described above, including compliance with legal, contractual, accounting, or reporting obligations.

When retention is no longer required, data will be securely deleted, anonymized, or archived in accordance with applicable law and internal data-retention schedules.

3.4 Automated Processing and Profiling

jenX does **not** engage in automated decision-making or profiling that produces legal or similarly significant effects on individuals.

3.5 Further Processing

If jenX intends to use Personal Data for a purpose materially different from that for which it was collected, we will provide prior notice and, where required by law, obtain your consent before such use.

4) Data Sharing and International Transfers

4.1 Disclosures to Service Providers and Partners

jenX Global Partners (“jenX”) shares Personal Data only as necessary to operate its business, fulfill contractual obligations, and comply with legal requirements. We do **not** sell or rent Personal Data to any third party.

Personal Data may be disclosed to the following categories of recipients:

- Cloud Hosting and IT Infrastructure Providers – for secure storage, hosting, and system administration (e.g., Amazon Web Services, Google Cloud).
- Communication and Productivity Platforms – for project management, messaging, scheduling, and collaboration (e.g., Slack, ClickUp, Google Workspace).
- Payment Processors and Financial Institutions – to facilitate billing and payments (e.g., Stripe, PayPal, domestic banks).
- Analytics and Advertising Partners – to analyze performance, improve user experience, and deliver targeted marketing (e.g., Google Analytics, Meta Ads, LinkedIn Ads).
- Recruiting, HR, and Payroll Vendors – to support the engagement, verification, and compensation of Virtual Assistants (VAs) and contractors.
- Professional Advisors and Auditors – to obtain legal, accounting, or compliance guidance.
- Authorities and Regulators – where disclosure is required by law, subpoena, or government request.

All such parties act as processors or sub-processors under written agreements requiring them to process Personal Data only on jenX’s instructions, maintain confidentiality, and implement appropriate technical and organizational safeguards.

4.2 Cross-Border Data Transfers

Because jenX operates internationally, Personal Data may be transferred to and processed in countries other than where it was collected – including the United States, the Philippines, and other jurisdictions in which jenX or its service providers maintain operations.

These locations may have data-protection laws that differ from those of your jurisdiction.

Where Partner or Connector data is transferred or accessed outside the individual’s country, including transfers to the United States or the Republic of the Philippines, such transfers are conducted under lawful data-transfer mechanisms and with appropriate safeguards.

Where Personal Data originates from the European Economic Area (EEA), United Kingdom, Switzerland, Canada, or Australia, jenX ensures that cross-border transfers occur only under appropriate safeguards consistent with applicable law, including:

- Execution of the European Commission’s Standard Contractual Clauses (SCCs) and, where applicable, the UK Addendum or International Data Transfer Agreement (IDTA);
- Implementation of supplementary technical and organizational measures (e.g., encryption, access controls, data-minimization); and
- Transfers to jurisdictions recognized by the European Commission or other authorities as providing an adequate level of data protection.

jenX continuously monitors regulatory guidance to maintain lawful transfer mechanisms for all international data flows.

4.3 Corporate Reorganizations and Business Transitions

If jenX undergoes a merger, acquisition, reorganization, sale of assets, or bankruptcy, Personal Data may be transferred as part of that transaction, subject to confidentiality protections and notice where required by law.

4.4 Legal Disclosures

jenX may disclose Personal Data when necessary to:

- Comply with applicable law or regulatory obligations;
- Respond to valid legal process or government requests;
- Protect the rights, property, or safety of jenX, our clients, users, employees, or the public; or
- Enforce our agreements and defend against legal claims.

5) Data Security and Retention

5.1 Security Measures

jenX Global Partners (“jenX”) implements administrative, technical, and physical safeguards designed to protect Personal Data from unauthorized access, alteration, disclosure, or destruction.

Such measures include, but are not limited to:

- Encryption of data in transit and at rest where technically feasible;
- Password-protected and access-controlled systems;
- Multi-factor authentication for administrative accounts;
- Network firewalls, intrusion detection, and endpoint protection;
- Role-based access management and principle of least privilege;
- Employee and contractor confidentiality agreements and security training; and
- Vendor due diligence and contractual data-protection obligations for all sub-processors.

jenX reviews and updates its information security practices periodically to align with industry standards and legal requirements.

5.2 Data Breach Response

In the event of an actual or suspected data breach, jenX will:

- Promptly investigate the incident and take appropriate mitigation steps;
- Notify affected clients or individuals without undue delay where required by law;
- Cooperate with regulators and provide any legally mandated reports; and
- Maintain documentation of the incident, actions taken, and lessons learned.

While jenX employs commercially reasonable security controls, no system can guarantee absolute security. Clients are responsible for maintaining the confidentiality of their account credentials and securing any systems under their control that interact with jenX Services.

5.3 Data Retention and Deletion

jenX retains Personal Data only for as long as necessary to:

- Fulfill the purposes described in Section 3 (How We Use Personal Data);
- Satisfy legal, accounting, or reporting obligations;
- Resolve disputes, enforce agreements, and protect jenX's rights; or
- Maintain business continuity, backup, and disaster recovery systems.

When retention is no longer required, Personal Data will be securely deleted, anonymized, or archived according to jenX's internal data-retention policy.

Clients may request deletion of their data at any time (see Section 7 – Individual Rights and Choices), subject to lawful exceptions or retention requirements. Data retention schedules are reviewed periodically to ensure alignment with business needs and legal requirements.

6) Data Transfers and Storage Locations

6.1 Primary Processing Locations

jenX Global Partners ("jenX") operates globally with primary data-processing activities occurring in:

- The United States – for business administration, client management, billing, marketing, and website hosting.
- The Philippines – for Virtual Assistant ("VA") and staffing operations, including communication, project coordination, and limited access to client data necessary for service delivery.
- Other Jurisdictions – where authorized service providers, cloud platforms, or contractors perform processing consistent with these Terms and this Privacy Policy.

All systems and platforms used for processing are hosted in secure data centers subject to contractual data-protection obligations and technical safeguards as described in Section 5.

6.2 Transfer Mechanisms

When Personal Data is transferred internationally – including between the EEA/UK/Switzerland/Canada/Australia and the United States or the Philippines – jenX relies on one or

more of the following lawful bases:

- Standard Contractual Clauses (SCCs) issued by the European Commission, together with the UK Addendum or International Data Transfer Agreement (IDTA) where applicable;
- Adequacy Decisions – for transfers to countries recognized as providing adequate data protection by the relevant authority;
- Contractual Necessity – where transfers are required to perform a contract with the data subject (e.g., VA placement or service delivery); or
- Explicit Consent – where clients or individuals affirmatively authorize a specific transfer after being informed of potential risks.

jenX conducts risk assessments for each international transfer, implements supplementary measures such as encryption and access controls, and maintains documentation of compliance with applicable data-transfer frameworks.

6.3 Data Localization and Access Controls

All Personal Data is logically segregated by client or project within jenX systems. Access is restricted to authorized personnel with a legitimate business need, following the principle of least privilege. jenX does not require clients to host data locally, but will comply with localization or residency requirements where mandated by applicable law or contract.

6.4 Ongoing Compliance and Review

jenX periodically reviews its cross-border transfer practices and updates its safeguards to reflect evolving regulatory standards, including new adequacy decisions, transfer frameworks (such as the EU–U.S. Data Privacy Framework), and national security assessments.

7) Individual Rights and Choices

7.1 Overview

Depending on your jurisdiction and applicable data-protection laws, you may have specific rights regarding your Personal Data. jenX Global Partners (“jenX”) will honor all rights granted by law to the extent required and feasible within the scope of our Services.

7.2 Rights of Data Subjects

Subject to verification and applicable legal limitations, you may exercise the following rights:

- Right of Access – to request confirmation of whether jenX processes your Personal Data and to obtain a copy of such data.
- Right to Rectification – to request correction of inaccurate or incomplete Personal Data.
- Right to Erasure (“Right to Be Forgotten”) – to request deletion of Personal Data where processing is no longer necessary or where consent has been withdrawn.

- Right to Restrict Processing – to limit how jenX processes your data in certain circumstances (e.g., during dispute resolution).
- Right to Data Portability – to receive your Personal Data in a structured, commonly used, and machine-readable format and to transmit it to another controller.
- Right to Object – to object to processing for direct marketing, profiling, or legitimate interests.
- Right to Withdraw Consent – where processing is based on consent, you may withdraw it at any time without affecting prior lawful processing.
- Right Not to Be Subject to Automated Decision-Making – jenX does not engage in fully automated decision-making that produces legal or similarly significant effects on individuals.

7.3 California Privacy Rights (CCPA/CPRA)

If you are a California resident, you have additional rights under the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), including:

- The right to know what categories of Personal Data jenX has collected, used, or disclosed in the preceding 12 months;
- The right to request deletion of your Personal Data, subject to lawful exceptions;
- The right to correct inaccurate information;
- The right to opt out of any “sale” or “sharing” of Personal Data (jenX does not sell data within the meaning of the CCPA); and
- The right not to be discriminated against for exercising your privacy rights.

California residents may designate an authorized agent to make requests on their behalf, provided sufficient proof of authorization and identity is supplied. California residents may also request a list of third parties to whom jenX has disclosed personal information for a business purpose in the preceding 12 months.

7.4 Exercising Your Rights

You may exercise any applicable data-protection rights by contacting:

Data Protection Officer (DPO)
 Attn: Jennie Largent
 Email: privacy@jenx.ai
 Mail: jenX Global Partners
 8407 Bandera Rd, Suite 103-271
 San Antonio, TX 78250, USA

jenX may request reasonable information to verify your identity before fulfilling a request. Responses will be provided within one (1) month (or as otherwise required by law).

7.5 Communication Preferences and Opt-Outs

You may opt out of receiving non-essential communications (such as marketing emails) by following the unsubscribe link in any message or by contacting us directly at privacy@jenx.ai.

Essential administrative or transactional emails related to your account, billing, or service delivery cannot typically be opted out of.

8) Data Controller, Data Protection Officer & Contact Information

8.1 Data Controller and Processor Roles

jenX Global Partners (“jenX”) acts as:

- Data Controller – when collecting and processing Personal Data for its own business purposes, such as client relationship management, billing, marketing, or recruitment; and
- Data Processor (or Service Provider) – when handling Personal Data on behalf of a client in connection with virtual assistant (“VA”) or staffing services, where the client determines the purposes and means of processing.

When acting as a processor, jenX processes Personal Data solely under the client’s written instructions, subject to appropriate contractual safeguards, and does not use or disclose such data for any purpose other than to provide the contracted Services.

8.2 Data Protection Officer (DPO)

jenX has appointed a Data Protection Officer to oversee compliance with this Privacy Policy and applicable data-protection laws.

Data Protection Officer (DPO)

Name: Jennie Largent

Email: privacy@jenx.ai

Mail: jenX Global Partners

8407 Bandera Rd, Suite 103-271

San Antonio, TX 78250, USA

The DPO is responsible for responding to privacy inquiries, investigating data incidents, managing compliance with cross-border transfer mechanisms, and serving as the primary contact for regulators and data subjects.

8.3 International Contact Points

For individuals located outside the United States, jenX recognizes and respects international privacy frameworks:

- European Union (EU) / United Kingdom (UK) – Data subjects may contact the DPO at privacy@jenx.ai with “EU/UK Privacy Inquiry” in the subject line. jenX will cooperate with competent supervisory authorities as required under Articles 27 and 31 of the GDPR.

- Canada – Inquiries may be addressed under the Personal Information Protection and Electronic Documents Act (PIPEDA).
- Australia – jenX adheres to the Australian Privacy Principles (APPs) for handling Personal Data and will cooperate with the Office of the Australian Information Commissioner (OAIC) if necessary.

8.4 Complaints and Regulatory Recourse

If you believe jenX has violated your privacy rights or mishandled your Personal Data, please contact the DPO first.

If your concern remains unresolved, you may have the right to lodge a complaint with the relevant data-protection authority in your jurisdiction, such as:

- The U.S. Federal Trade Commission (FTC) – www.ftc.gov
- Your local EU/EEA Data Protection Authority – <https://edpb.europa.eu>
- The UK Information Commissioner’s Office (ICO) – www.ico.org.uk
- The Office of the Privacy Commissioner of Canada (OPC) – www.priv.gc.ca
- The Office of the Australian Information Commissioner (OAIC) – www.oaic.gov.au

9) Updates, Notifications, and Version Control

jenX Global Partners (“jenX”) may update or amend this Privacy Policy from time to time to reflect changes in legal requirements, technological advancements, business operations, or industry best practices.

When updates occur:

- The “Last Updated” date at the top of this Policy will be revised;
- The updated Policy will be posted on jenx.ai/privacy (or its successor URL); and
- In cases of material changes – such as introducing new data uses, sharing practices, or lawful bases – jenX will provide additional notice, which may include email communication, website banners, or in-platform alerts.

By continuing to use our Services after a revised version is posted or after being notified of material changes, you acknowledge and agree to the updated terms of this Privacy Policy.

If you do not agree with any changes, you should discontinue use of the Services and contact privacy@jenx.ai to request deletion of your account or associated Personal Data, subject to applicable legal retention requirements.

The Effective Date identifies when the most recent version of this Privacy Policy took effect, and the Last Updated date indicates when the text was most recently revised.

10) Effective Date, Interpretation & Contact Summary

10.1 Effective Date

This Privacy Policy is effective as of October 24, 2025. It supersedes all prior versions or statements concerning jenX Global Partners' data-protection practices.

10.2 Interpretation

Headings and section titles in this Privacy Policy are for convenience only and do not affect interpretation. Any undefined capitalized terms have the meaning given in the Terms of Service.

This Privacy Policy is intended to be interpreted broadly to ensure compliance with applicable laws, including but not limited to:

- The General Data Protection Regulation (EU) 2016/679 (GDPR) and UK GDPR;
- The California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA);
- The Personal Information Protection and Electronic Documents Act (PIPEDA) (Canada); and
- The Australian Privacy Act 1988 and Australian Privacy Principles (APPs).

If any provision of this Policy is found to be invalid or unenforceable, the remaining provisions shall remain in full force and effect.

10.3 Contact Summary

For questions, privacy requests, partner inquiries, or complaints, please contact:

Data Protection Officer (DPO)

Attn: Jennie Largent

Email: privacy@jenx.ai

Mail: jenX Global Partners

8407 Bandera Rd, Suite 103-271

San Antonio, TX 78250, USA

Phone: +1 (210) 595-0415

Approved by: Jennie Largent, Data Protection Officer, jenX Global Partners

Version History

Version	Effective Date	Summary of Changes
1.0	10/24/2025	Initial publication of Privacy Policy