

PRIVACY POLICY

Involute Inc. d.b.a. Xuno

Effective Date: June 16, 2026

In relation to the products and services provided under its brands and subsidiaries.

This privacy policy ("Policy") describes how Involute Inc. d.b.a Xuno ("Company", "we", "us", or "our") may collect, use, process, transfer, store and retain your Customer Data and with whom and for what purposes we may share your Customer Data. This Policy applies to both individual consumers and business customers (including sole proprietors, partnerships, corporations, and other legal entities) who access or use our services. There may be additional regulations and standards that apply to your Customer Data depending on the country or region in which you reside or any Applicable Laws.

1. Definition of Terms

The following terms used in this Policy shall have the meaning given to them below unless the context requires otherwise:

Applicable Laws:

Means any laws, rules, bylaws, regulations, decrees, enactments, orders, mandates, or resolutions promulgated by legislative or other authorized government entities relating to data, data security, data protection, data privacy, and data processing that apply to us and our services.

Business Customer:

Means any legal entity, including but not limited to corporations, limited liability companies, partnerships, sole proprietors operating under a business name, or any other legally recognized commercial entity, that registers for or uses the Company's services for commercial or business purposes.

Individual Customer:

Means any natural person who registers for or uses the Company's services in their personal capacity, including senders and recipients of payments who access the services as individual consumers rather than as a Business Customer. Where an Individual Customer is legally incapacitated, their Authorized Representative (such as a parent, guardian, or attorney-in-fact) may act on their behalf, subject to applicable law. Our services are not intended for use by individuals under the age of 18; please refer to Section 9 for details.

Authorized Representative:

Means a natural person who is duly authorized to act on behalf of another party in connection with the Company's services. This includes: (a) in the context of an Individual Customer, a person holding a valid power of attorney, legal guardianship, or other legally recognized authority to act on behalf of that individual (for example, a guardian acting for a minor or an incapacitated person); and (b) in the context of a Business Customer, an employee, officer, director, or agent duly authorized by the Business Customer to execute agreements, submit documentation, manage the account, and otherwise interact with the Company's services on the Business Customer's behalf.

Customer Data:

Means personal data and other data relating to you (whether an individual or a Business Customer) as defined under Applicable Law. This typically includes any information relating to you and your transactions as described in this Policy. For Business Customers, Customer Data also includes business information, financial records, and data relating to Authorized Representatives and beneficial owners.

Company:

Means Involute Inc. d.b.a. Xuno and its references to "we", "our", "us".

You or Your:

Means (a) an individual who is a visitor to one of our websites or mobile apps, or a user or recipient of our services; or (b) a Business Customer accessing or using our services, in which case this Policy binds the Business Customer and applies to the Authorized Representatives and personnel who interact with our services on the Business Customer's behalf.

2. Types of Customer Data We May Collect

We collect Customer Data from and about our users, including both Individual Consumers and Business Customers. This section provides non-exhaustive examples of Customer Data we collect, subject to the country or region in which you are located and Applicable Laws. Some data may be deemed sensitive under laws of certain jurisdictions and may not be collected in those regions.

2.1 Individual Customer Data

For individual users, we may collect:

- * Name, email address, and phone number when you create your account.
- * Address, date of birth, and demographic information (such as gender and marital status) when you complete your profile.
- * Biometric authentication confirmation (via your device's Face ID or fingerprint sensor) if you opt into biometric login (optional). Biometric processing happens locally on your device; we do not collect or store your photo, image, or raw biometric data.
- * GPS location automatically when you initiate a transaction. We collect this data solely to fulfill regulatory and fraud prevention obligations. Collection is limited to the moment of transaction initiation and is not used for continuous tracking.
- * Financial information (such as account holder name, bank name, account type, and routing/account number) when you link your bank account.
- * Transaction information (such as payment amount, date, recipient details, relationship to the recipient, and purpose of transaction) when you initiate a transaction.
- * Device identifier for any device used to access our online services (such as model, serial number, and usage tracking) automatically upon log-in and when you initiate a transaction.
- * Cookies and other tracking technology data automatically when you visit our website or app. Please refer to Section 7 (Cookie Policy) for full details.
- * Usage data such as time and duration of use, error reports, and performance data, including your IP address and related metadata, automatically upon log-in.
- * Type and version of your device's operating system or web browser when you visit our website or app.

2.2 Business Customer Data

For Business Customers, we may collect the following categories of data in addition to, or instead of, the Individual Customer Data listed above:

Business Identity and Registration Information:

- * Legal business name, trade name (d.b.a.), business type, and jurisdiction of formation.
- * Employer Identification Number (EIN) or Tax Identification Number (TIN), and other government-issued identifiers.
- * Certificates of incorporation, articles of organization, business licenses, or equivalent formation documents.

- * Registered business address and/or principal place of business.

Beneficial Ownership and Authorized Representative Information:

- * Names, dates of birth, nationalities, and government-issued identification documents of beneficial owners (i.e., individuals who own or control 25% or more of the business entity, or who exercise control).
- * Name, contact details, and authorization credentials of Authorized Representatives acting on behalf of the Business Customer.
- * Percentage of ownership and nature of control for each beneficial owner.

Business Financial Information:

- * Business bank account details, including account holder name, account number, and routing number.
- * Business transaction information, including payment amounts, frequency, counterparty details, purpose of payment, and bulk transfer instructions.

Know Your Business (KYB) Documentation:

- * Proof of business address (e.g., utility bills, lease agreements, government correspondence, bank statements).
- * Audited or unaudited financial statements where required by Applicable Law or our compliance framework.
- * Industry classification and a description of business activities.
- * Information about the business's customers, counterparties, and jurisdictions of operation where relevant for risk assessment.

Operational and Usage Data:

- * IP addresses and device identifiers used by Authorized Representatives to access the business account.
- * Log data associated with business account activity, including transaction submissions, approvals, and administrative actions.
- * Bulk transfer files and associated recipient data submitted by the Business Customer.

3. Our Use, Processing, and Sharing of Customer Data

We use, process and share Customer Data, including with affiliated payment processors, banks, financial institutions, and third-party service providers, where we have a legal basis to do so. The legal bases include the performance of a contract, compliance with regulatory obligations, and pursuit of legitimate business interests.

3.1 Contract Performance

One of the primary legal grounds for using, processing, and sharing Customer Data is the contract entered into between you and us. Activities carried out pursuant to this include:

- * Creation and management of individual and business accounts.
- * Origination and processing of payment instructions, including bulk transfers for Business Customers.
- * Provision of payment services as set out in the applicable terms of use.
- * Maintaining your access to related services and sending you communications regarding the services, maintenance, functionality, or other relevant matters.
- * Any other purpose for which we obtain your prior consent before using your Customer Data.

3.2 Regulatory Compliance

We use, process, and share Customer Data to comply with our regulatory obligations, including:

- * KYC (Know Your Customer) and KYB (Know Your Business) obligations, including ongoing due diligence and periodic reviews of both Individual Customer and Business Customer accounts.
- * AML (Anti-Money Laundering) and CFT (Combating the Financing of Terrorism) obligations, including transaction monitoring and suspicious activity reporting.
- * Beneficial ownership verification in accordance with FinCEN requirements and equivalent regulations in other jurisdictions.
- * OFAC and international sanctions screening for both individual and Business Customers, Authorized Representatives, and beneficial owners.
- * Regulatory reporting obligations to financial regulators, law enforcement agencies, and government authorities where required by Applicable Law.

3.3 Legitimate Business Interests

Subject to Applicable Law, we may collect, use, process, and share Customer Data to pursue our legitimate business interests, including:

- * Improving our services, systems, and user experience.
- * Updating our systems, tools, and services.
- * Promoting and growing our services and user base.
- * Collaborating with third parties to operate our business, including sharing Customer Data subject to contractual data protection obligations.

3.4 Sharing with Third Parties

The Company may share Customer Data with third parties for the following purposes:

- * Third-party service providers performing specialized services for the Company, where such use is governed by a data processing agreement limiting their use of Customer Data to the specified purpose.
- * Third parties assisting the Company in providing its services, subject to contractual data protection obligations.
- * Regulators, courts, law enforcement agencies, and governmental authorities, to comply with Applicable Laws, court orders, and lawful requests.
- * KYB, KYC, and identity verification service providers engaged for onboarding and ongoing due diligence of both individual and Business Customers.
- * In the event of a business reorganization, merger, acquisition, or sale of assets, potential or actual acquirers, who will have the right to continue using Customer Data in compliance with the terms of this Policy.

3.5 Applicable Privacy Framework

The processing of Customer Data under this Policy is governed by applicable privacy and data protection laws based on where you reside and where the Company operates. This applies equally to Individual Customers and Business Customers.

For Individual Customers and Business Customers based in the United States, the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), applies to California residents. Other US state privacy laws may also apply depending on your state of residence. Our practices are designed to comply with applicable US federal and state privacy obligations across all customer types.

For Individual Customers who are recipients of payments processed through our services, the data protection laws of the recipient's country of residence may apply to the processing of their personal data. We comply with all such Applicable Laws in the jurisdictions in which we operate.

4. International Transfers of Customer Data

We operate in multiple jurisdictions. Accordingly, your Customer Data may be stored and processed in any country where we operate. We may transfer your Customer Data to a country other than your country of residence or nationality. While carrying out cross-border transfers of data, we comply with all Applicable Laws. Prior notice will be provided and consent will be obtained where required.

5. Data Retention, Security, and Breach Notification

5.1 Data Retention

We will retain your Customer Data for as long as necessary to comply with applicable law, fulfill any ongoing obligations to you, or for our internal business purposes, where consistent with Applicable Law.

We may retain your Customer Data even after you close your Company account or request deletion of your personal information. Examples of such cases include:

- * To process any transactions initiated prior to the closure or deactivation of your account.
- * To comply with anti-money laundering regulations or other legal requirements.
- * To detect or prevent fraud, unauthorized activity, or other loss prevention measures.
- * To comply with legal processes, court orders, regulatory requests, or law enforcement inquiries.
- * To recover any fees or other outstanding amounts owed to the Company.
- * To comply with tax, accounting, financial, and regulatory reporting obligations.
- * Where required by contractual commitments to our partners within the Company ecosystem.
- * To resolve disputes or enforce our User Agreement or other applicable agreements or policies.
- * To exercise any other rights or take actions permitted under applicable law.
- * To retain records for periods required to comply with legal and regulatory retention obligations (which typically require retention of transaction records for a minimum of five years).

Once the relevant retention period has expired, the Company will securely destroy your Customer Data or, where applicable, anonymize it so that it can no longer be associated with you.

5.2 Data Security

We make reasonable efforts to keep Customer Data secure. Our security measures include administrative, technical, and organizational safeguards designed to protect Customer Data against unauthorized access, loss, misuse, disclosure, alteration, or destruction. These include:

- * Encryption of Customer Data in transit and at rest.
- * Access controls and role-based permissions limiting data access to authorized personnel.
- * Regular security assessments and vulnerability monitoring.
- * Incident response procedures.

Data Breach Notification:

In the event of a data breach that is likely to result in harm to you, whether as an Individual Customer or a Business Customer, we will notify affected parties and relevant regulatory authorities within the timeframes required by Applicable Law, including applicable US federal and state breach notification requirements, as well as the obligations of any other jurisdiction in which we operate. Notification will be provided via the contact details you have on file with us.

Please note that no security system can guarantee 100% protection. If you believe your Customer Data or interactions with us are no longer secure, please contact us immediately using the details in Section 11 (Contact Us).

6. Updates to This Policy

We may update this Policy from time to time for various reasons, including to comply with Applicable Law, to reflect changes in our data practices, or to incorporate requirements of new services we may offer.

The date at the top of this document reflects when this Policy was last updated. We will notify customers who use our services of material updates via the email they have provided. We may also post alerts on our websites and mobile apps.

Where required by Applicable Law or relevant authorities, we will obtain your consent or provide notice in the specified manner prior to making changes that materially affect how we process your Customer Data. Business Customers will be notified through the contact details of their Authorized Representative on file.

7. Cookie Policy

We use cookies and similar tracking technologies (including web beacons, pixel tags, and local storage) to collect Customer Data as described in this Policy. This section explains how we use these technologies.

Categories of Cookies We Use:

- * **Strictly Necessary Cookies:** Required for the operation of our website and services. These cannot be disabled without affecting core functionality, such as authentication and transaction processing.
- * **Analytics and Performance Cookies:** Used to understand how visitors interact with our website and services (e.g., pages visited, error messages, load times). This data is aggregated and does not identify individuals.
- * **Targeting and Advertising Cookies:** Used with your consent to deliver relevant content and assess the effectiveness of our communications. We do not currently sell your data to advertisers, but we may use analytics partners to understand usage trends.

8. Third-Party Links

Our platform may incorporate or embed third-party integrations or third-party branded services ("Third-Party Services"). Enabling or interacting with these Third-Party Services may allow third parties to collect or share information about you. The Company does not own or control these Third-Party Services, and when you engage with them, you may be providing information directly to the third party, to the Company, or to both. Each Third-Party Service has its own policies governing the collection, use, and disclosure of your information and the Company is not responsible for any third-party privacy policies and practices. We encourage you to review those policies before engaging with any Third-Party Service through our platform.

To protect our online resources and services against malicious activity, we use Cloudflare Turnstile, a pro-privacy website security tool designed to distinguish human users from bots and block bot traffic. Your use of this feature is subject to Cloudflare's Turnstile Privacy Policy.

9. Children's Data

Our services are not intended for use by individuals under the age of 18. We do not knowingly collect personal data from individuals under 18. If you are under 18, please do not use our services or provide any personal data through them.

If we become aware that we have inadvertently collected personal data from a child under 13 (or under 18 where required), we will take steps to delete that data promptly. If you believe we may have collected such data, please contact us using the details in Section 11.

10. Your Rights and Control Over Your Customer Data

Your rights over your Customer Data vary depending on your country, region, and Applicable Law. These rights are available to both Individual Customer and Business Customers (exercised through an Authorized Representative).

General Rights (where applicable):

- Right to access:** Request a copy of the Customer Data we hold about you.
- Right to rectification:** Request correction of inaccurate or incomplete Customer Data.
- Right to erasure:** Request deletion of your Customer Data, subject to our legal retention obligations.
- Right to restriction:** Request that we limit the processing of your Customer Data in certain circumstances.
- Right to data portability:** Receive your Customer Data in a structured, machine-readable format where technically feasible.
- Right to object:** Object to processing based on legitimate interests or for direct marketing purposes.
- Right to withdraw consent:** Where processing is based on your consent, withdraw it at any time without affecting the lawfulness of prior processing.

We will comply with your request as soon as reasonably practicable and within the timeframes required by Applicable Law. We may be unable to fulfill a request if we no longer hold the relevant Customer Data or if a legal obligation requires us to retain it.

If you are not satisfied with how we handle your request, you may have the right to lodge a complaint with the data protection authority of your jurisdiction under Applicable Law.

11. Contact Us

If you have any questions, complaints, or if you wish to exercise any of the rights described in this Policy, please contact us:

Phone: 1-866-356-1201
Email: info@xuno.co
Postal Address:
Involute Inc. d.b.a. Xuno
2108 W Clearview Dr
Ellensburg, WA 98926

Please note that we may require you to verify your identity before complying with your request. If you wish to use an authorized agent to submit a request on your behalf (including an Authorized Representative for Business Customers), we will require written authorization confirming that the agent has been granted permission to act. We may deny a request if identity or authorization cannot be verified.

12. Electronic Fund Transfers (EFTs) and Account Balances

Involute Inc. d.b.a. Xuno partners with financial services software company Sila Inc. ("Sila") and the financial services partner, Priority Commerce, who assist with electronic fund transfers and banking services. By registering for our platform, linking your external bank account, and authorizing any electronic payment, you authorize us to share your identity and banking information with Sila Inc. and Priority Commerce to support your Account. You also agree to the terms and conditions of [Sila's privacy policy](#) and [Priority Commerce's privacy policy](#) (the "Partner Privacy Terms"). It is your responsibility to ensure the data you provide to us is accurate and complete, which is necessary for our partners to process electronic fund transfers on your behalf and provide you with continued access to the Account. The Partner Privacy Terms may be modified from time to time, and the governing versions are incorporated by reference as part of this Privacy Policy. IT IS YOUR RESPONSIBILITY TO READ AND UNDERSTAND THE PARTNER PRIVACY TERMS BECAUSE THEY CONTAIN TERMS AND CONDITIONS CONCERNING YOUR ACCOUNT WITH US, INCLUDING BUT NOT LIMITED TO USE OF YOUR PERSONAL INFORMATION.

13. Specific Provisions for Specific Jurisdictions

The following provisions supplement the rest of this Policy for customers in specific jurisdictions. In the event of a conflict between these jurisdiction-specific provisions and the general provisions of this Policy, the jurisdiction-specific provisions shall take precedence for customers in the relevant jurisdiction.

13.1 California. California Consumer Privacy Act (CCPA/CPRA)

If you are a resident of the State of California, you have the following rights under the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA):

Exercising the Right to Know.

You may request, up to twice in a 12-month period, information about the personal information collected about you in the past 12 months, including: (a) categories and specific pieces collected; (b) categories of sources; (c) business or commercial purpose for collection; (d) categories of third parties with whom it was shared; and (e) categories disclosed for a business purpose.

Exercising the Right to Delete.

You may request deletion of personal information we have collected from you, subject to certain exceptions under Applicable Law (including our legal retention obligations).

Exercising the Right to Opt-Out of Sharing.

You may request to opt-out of sharing your personal information for cross-context behavioral advertising.

Non-Discrimination.

The CCPA provides that you may not be discriminated against for exercising these rights.

To submit a request to exercise any of the rights described above, contact Involute Inc. d.b.a. Xuno either by email to info@xuno.co or contact us via postal mail, proper postage prepaid, at:

Involute Inc. d.b.a. Xuno
Attn: Your California Privacy Rights

**2108 W Clearview Dr
Ellensburg, WA 98926**

Please indicate your preferred response method (email or postal mail). All postal requests must be labeled "Your California Privacy Rights" on the envelope and must include your full name, street address, city, state, and zip code. We may verify your identity before responding. Authentication based on a government-issued identification document may be required. We will not accept requests via telephone or fax. We are not responsible for requests that are not properly labeled, incomplete, or sent to the wrong address.

13.2 Nepal. Individual Privacy Act (IPA) and Applicable Nepalese Law

Nepalese law requires that we disclose to you the purpose for which we collect your Customer Data and that we not use the Customer Data for any purpose other than what is disclosed to you. Nepalese law further requires, for certain types of Customer Data, that we disclose the time, the subject, and the nature of data being collected; the purpose of collection, and the provisions relating to the security of the data. If you are a customer in Nepal, we will collect and process your Customer Data in compliance with this requirement.