Knetyc Corporation Privacy Policy

Effective Date: October 28, 2026

At Knetyc Corporation ("Knetyc," "we," "us," or "our"), we value your privacy and are committed to protecting your personal information. This Privacy Policy explains how we collect, use, share, and safeguard personal information when you use our website, Knetyc.com, our web application, the Knetyc Model Context Protocol server (the "Knetyc MCP Server"), any application programming interface we make available, our AI chat support tool, and related services (collectively, the "Service"), and when you otherwise interact with us, such as by communicating with us or attending our events. Capitalized terms not defined here have the meanings given in our Terms of Service.

Our Service is designed for businesses and professionals. When a company or other organization (a "Customer") provides the Service to its employees and contractors under an enterprise subscription, pilot, or other written agreement, we process the personal information contained in that Customer's Content on the Customer's behalf and under its instructions, as its service provider or processor. In that case, the Customer's own privacy notice and our agreement with the Customer govern that processing, and you should direct questions and requests about it to the Customer. This Privacy Policy describes our practices as a business or controller, and also describes how we handle Customer Content generally.

1. Information We Collect

We collect information to provide and improve the Service. The types of information we collect include:

1.1 Information You Provide

- **Account Information:** When you create an account or are invited to an organization account, we collect your name, company name (if applicable), job title, email address, and phone number, as well as your organization membership, role, and permissions. Payment details (e.g., credit card, debit card, or ACH information) are collected by a third party vendor, and we do not have access to such information; we receive only limited information from the vendor, such as the card type, last four digits, billing address, and transaction status.
- **User Content:** We collect building plans, site plans, specifications, and related documents you upload to the Service for analysis; questions and prompts you submit; site addresses, parcel identifiers, and project information; plan-review comments you paste or upload; and documents you add to an Organization Workspace. User Content is typically technical and business information, but it may contain personal information, such as the names, license numbers, and contact details of design professionals, owners, or reviewers that appear on plans and correspondence. We also collect text of conversations with the Knetyc AI chat support tool on the website.
- **Communications:** Information you share when you contact us, such as through support inquiries, feedback, surveys, sales discussions, or event registrations.

1.2 Information We Receive Through MCP Clients

When you or your organization connect an MCP Client to the Knetyc MCP Server, we receive information that the MCP Client sends to us when it calls our tools on your behalf. This includes the identifiers and access tokens issued when you authorize the connection, the name and version of the MCP Client, the tools called and the inputs provided to them (such as your questions, jurisdiction and project details, pasted comments, and files transferred through download links that the MCP Client authorizes), request identifiers and timestamps, and records of the AI model usage associated with each request. We do not receive your full conversation with the MCP Client, only the information the MCP Client includes in its requests to us. The provider of your MCP Client collects and processes your conversations, files, and the Output we return under its own privacy policy, and we are not responsible for its practices.

1.3 Information Collected Automatically

- **Usage Data:** We collect data about your interactions with the Service, including your IP address, browser type, device information, pages visited, features and tools used, timestamps, and log, error, and audit records (such as records of uploads, analyses, exports, sharing, and deletions).
- **Cookies and Tracking Technologies:** We use cookies and similar technologies to enhance your experience, such as keeping you logged in and analyzing usage patterns. See Section 6 for details.

1.4 Information from Third Parties and Public Sources

We may receive information from third-party services (e.g., payment processors, single sign-on and identity providers, and MCP Client providers during authorization) to facilitate transactions or verify your account details, and from your organization when an administrator invites you or manages your account. To generate Output, the Service retrieves information from public sources, such as published codes and ordinances, government websites, zoning and geographic information system data, and parcel and property records; these sources may include personal information, such as the names of property owners associated with a parcel, which we process only as needed to produce the analysis you request. We may also collect business contact information about professionals from publicly available sources, such as company websites, and from event organizers, to communicate with prospective customers. Other than as described in this Section, we do not collect data from public or commercial sources unless explicitly authorized by you.

2. How We Use Your Information

We use your information to:

- Provide and maintain the Service, including processing your uploaded documents, researching codes and site information, and generating analysis through our AI Features.
- Enable organization accounts, including user management, sharing, permissions, and administrator visibility into usage.
- Authenticate users and MCP Clients, process tool requests, and enforce entitlements, quotas, and usage limits.
- Process payments and manage your subscription or enterprise account.
- Respond to your inquiries, provide customer support, and address technical issues.

- Improve the Service by analyzing usage trends and statistics, de-identified information about the quality and accuracy of Output, and user feedback, without using Customer Content to train AI models (see Section 3).
- Prepare de-identified Jurisdiction Insights as described in Section 3.
- Send you Service-related communications, such as billing reminders, renewal notices, or account updates, and, where permitted, information about our products, from which you may opt out at any time.
- Protect the security and integrity of the Service, including detecting and preventing fraud, abuse, prompt injection, and unauthorized access.
- Comply with legal obligations or enforce our Terms of Service.

3. Artificial Intelligence and Your Data

- **AI model providers:** The Service uses AI models provided by third parties to analyze Content and generate Output. We send these providers only the information needed to perform the requested analysis, and we require them by contract to process it solely to provide services to us, to protect it, and not to use it to train or improve their models. Some providers may retain inputs and outputs for a limited period to detect abuse, as permitted by their agreements with us.
- **No training on your content:** We do not use Customer Content or Output to train, fine-tune, or otherwise develop AI models, whether ours or a third party's.
- **Large language model training disclosure:** We do not collect, use, or sell personal data for the purpose of training large language models.
- **Jurisdiction Insights:** When plan-review or other comments issued by an authority having jurisdiction are submitted to the Service, we may prepare jurisdiction-level summary information about that authority's review practices and code interpretations. We recast the information as summary information and remove the identity of the Customer, its users, the project, the site, and any other individual, so that it is completely anonymized. Jurisdiction Insights are used only as background information to inform analyses for any user and are never quoted, cited, or specifically referred to in Output provided outside the submitting organization. Project documents that contain agency comments remain available for citation only in analyses performed for users within the organization that uploaded them. An enterprise agreement may exclude a Customer's Content from use in preparing Jurisdiction Insights.
- **No automated decisions about individuals:** We do not use automated decision-making technology or profiling to make decisions that produce legal or similarly significant effects concerning individuals. Output is an informational aid for professional review of projects and sites.
- **AI interactions:** Our chat support tool and AI Features use generative AI. When you interact with them, you are interacting with AI and not a human, unless we tell you otherwise.

4. How We Share Your Information

We do not sell your personal information, and we do not share it for cross-context behavioral advertising or targeted advertising. We may share your information in the following circumstances:

- **Service Providers:** We share information with trusted third-party providers who assist in operating the Service, such as cloud hosting and data storage providers (e.g., Google Cloud and Firebase), AI

model providers, email and productivity providers (e.g., Google Workspace), payment processors, customer relationship management and support tools, and security and analytics providers. They are subject to written agreements requiring them to protect the information, keep it confidential, and use it only to provide services to us. A current list of subprocessors that process Customer Content is available on request at legal@knetyc.com. Enterprise agreements may require us to maintain a register of these providers and to give a Customer advance notice of, or obtain its approval for, new providers that process its Content.

- **Within Your Organization:** If you use an organization account, your name, email address, role, activity, and the Content and Output you place in the Organization Workspace or shared projects may be visible to your organization's administrators and other Authorized Users according to the permissions your organization assigns.
- **At Your Direction:** We share information with third parties when you direct us to, such as when you connect an MCP Client and it requests Output, or when you export or share a report.
- **Legal Compliance:** We may disclose information to comply with applicable laws, regulations, or legal processes, or to respond to lawful government requests.
- **Business Transfers:** In the event of a merger, acquisition, financing, or sale of assets, your information may be transferred as part of the transaction, with notice to you where required.
- **Protection of Rights:** We may share information to enforce our Terms of Service, protect our rights, or prevent illegal activities.
- **Aggregated or Anonymized Data:** We may share non-identifiable, aggregated data, including Jurisdiction Insights and industry statistics, for research, analytics, or benchmarking purposes. We will not attempt to re-identify de-identified information, and we contractually prohibit recipients from doing so.

5. Data Security

We take reasonable measures to protect your information, including:

- Storing data with established cloud providers, including Firebase and Google Workspace, relying on their encryption and access controls, with data encrypted in transit and at rest.
- Implementing industry-standard security protocols to prevent unauthorized access or disclosure, including role-based access controls, organization-level data separation, and server-side verification of each user's permissions.
- Securing MCP access through authorization tokens that you can revoke, request validation, rate and concurrency limits, and short-lived, time-limited links for file transfers and report downloads.
- Maintaining audit records of significant actions, such as uploads, analyses, exports, sharing, and deletions.
- Conducting regular security reviews to address potential vulnerabilities, and reviewing the security practices of our service providers.

While we strive to protect your data, no online service is completely secure. We cannot guarantee absolute security. If we become aware of a security incident affecting your personal information, we will notify you and others as required by applicable law.

6. Cookies and Tracking Technologies

We use cookies and similar technologies to:

- Authenticate your account and keep you logged in.
- Track usage patterns to improve the Service.
- Personalize your experience, such as remembering your preferences.

We do not use cookies for cross-context behavioral advertising. You can manage cookies through your browser settings or opt out of non-essential cookies by contacting us directly. We honor Global Privacy Control and similar browser-based opt-out preference signals where required by applicable law. Disabling cookies may affect certain features of the Service.

7. Data Retention

We retain your personal information and User Content for as long as your account is active or as needed to provide the Service. When an account or enterprise agreement ends, you may request an export of Content for thirty (30) days, after which we delete or de-identify User Content from our active systems within ninety (90) days, and from backups as they are overwritten in the ordinary course, within an additional ninety (90) days. When you or an administrator delete a document from an Organization Workspace, it is immediately withdrawn from use and information derived from it is invalidated; we retain the original file and related audit records for up to ninety (90) days to protect the integrity and security of the Service and to permit recovery of accidental deletions, unless a longer period is required by law or an enterprise agreement. We retain MCP request and usage records and security logs for up to twenty-four (24) months. We may also retain data to comply with legal obligations, resolve disputes, or enforce our agreements. We may also retain data to perform anonymized and/or aggregated statistical analyses to strengthen the Service and to generate information about industry trends, and we retain Jurisdiction Insights and other anonymized information indefinitely. You may request deletion of your account and associated data by contacting us at legal@knetyc.com, subject to any legal retention requirements. If you use the Service under an enterprise agreement, the export, retention, and deletion periods in that agreement control over this Section.

8. Your Privacy Rights

Depending on your location (e.g., U.S. states with comprehensive privacy laws, such as California, Colorado, Connecticut, Indiana, Kentucky, Oregon, Rhode Island, Texas, Utah, and Virginia, or jurisdictions like Canada), you may have certain rights regarding your personal information, including:

- **Access:** Confirm whether we process your personal information and request a copy of the personal information we hold about you, including the categories of personal information and of third parties to which we have disclosed it.
- **Correction:** Request correction of inaccurate or incomplete information.
- **Deletion:** Request deletion of your personal information, subject to legal retention obligations.
- **Opt-Out:** Opt out of the use of your data for marketing communications, and of the sale of personal information, targeted advertising, and profiling in furtherance of decisions that produce legal or similarly significant effects. As described above, we do not engage in these activities.

- **Portability:** Request your data in a structured, commonly used format (where feasible).
- **Appeal:** If we decline to take action on your request, you may appeal our decision by replying to our response or emailing legal@knetyc.com with the subject line "Privacy Appeal." We will respond to your appeal within the time required by law. If you are not satisfied, you may contact your state attorney general or other applicable regulator.
- **Non-Discrimination:** We will not discriminate against you for exercising your privacy rights.

To exercise these rights, please contact us at legal@knetyc.com. We will need to verify your identity before responding, which may require you to confirm information associated with your account. You may use an authorized agent to submit a request on your behalf where permitted by law, and we may ask the agent to provide proof of authorization. If your personal information is held in an organization account under an enterprise agreement, we may refer your request to that organization. We will respond within the timeframes required by applicable law (e.g., 30 days under PIPEDA or 45 days under CCPA and most other U.S. state privacy laws, which may be extended where permitted).

8.1 Additional U.S. State Privacy Disclosures

In the preceding twelve months, we have collected the following categories of personal information, from the sources described in Section 1, for the purposes described in Sections 2 and 3: identifiers (such as name, email address, phone number, IP address, and account and MCP connection identifiers); professional or employment-related information (such as company, job title, organization role, and professional license information appearing in Content); commercial information (such as subscription and transaction records); internet or other electronic network activity information (such as Usage Data and audit records); approximate geolocation derived from IP address; and the contents of communications and Content you submit to the Service. We disclose each of these categories for business purposes to the service providers and other recipients described in Section 4. We do not collect sensitive personal information for the purpose of inferring characteristics about individuals, and we do not knowingly sell or share the personal information of consumers under 18 years of age.

9. Children's Privacy

The Service is not intended for individuals under 18 years of age. We do not knowingly collect personal information from children. If we learn that we have collected such information, we will take steps to delete it promptly. Please contact us if you believe we have inadvertently collected data from a child.

10. International Users

The Service is operated from the United States and hosted on servers in the U.S. Our service providers, including AI model providers, may process information in the U.S. and other countries. If you access the Service from outside the U.S., including Canada, your data will be transferred to and stored in the U.S., where it may be accessible to courts, law enforcement, and national security authorities under U.S. law. By using the Service, you consent to this transfer and processing, subject to applicable privacy laws. If you are in Quebec, you acknowledge that your personal information may be communicated outside Quebec for the purposes described in this Privacy Policy.

11. Third-Party Services

The Service may link to or interoperate with third-party services, including MCP Clients, single sign-on providers, and websites we cite in Output. Their collection and use of information is governed by their own privacy policies, and we encourage you to review them.

12. Changes to This Privacy Policy

We may update this Privacy Policy to reflect changes in our practices or legal requirements, and we will update the "Last Updated" date at the top of this policy when we do. We will notify you of material changes by posting the updated policy on the Service or sending you an email at least 30 days before the changes take effect. Your continued use of the Service after the effective date constitutes your acceptance of the updated policy. We will obtain your consent before using previously collected personal information in a materially different way where required by law.

13. Contact Us

If you have questions, concerns, or requests regarding this Privacy Policy or our data practices, please contact us at:

Knetyc Corporation

Email: legal@knetyc.com

Website: Knetyc.com

We will respond to your inquiries promptly and in accordance with applicable law.