**PRIVACY NOTICE**

*Effective Date: May 27, 2025*



## Introduction

This Privacy Notice explains how **Archiki OÜ** ("**Archiki**," "**we**," "**us**," or "**our**") collects, processes, uses, discloses, and protects your personal data.

We are committed to:

- Providing clear and easily accessible information on how we handle your personal data.
- Implementing technical and organizational measures to safeguard your data from unauthorized access, loss, or misuse.
- Complying with applicable data protection regulations.
- Enabling you to manage your privacy settings and exercise your rights.

This Privacy Notice applies when you interact with us in any of the following ways:

- Access and use our Platform, located at www.archiki.com, and related services, as a registered user, visitor, or prospective customer.
- Visit our site www.archiki.com and other sites operated by us (**"Website"**) that reference this Privacy Notice.
- Engage with us on social media, including posts, discussions, and communication through our social media channels.

- Attend events hosted by us, such as webinars, workshops, or in-person events.
- Interact with us as a business contact or prospect in the context of inquiries, eligibility assessments, or business development.
- Receive marketing communications, such as newsletters or updates, where permitted by law.
- Communicate with our support, sales, or customer success teams for assistance or inquiries.
- Participate in surveys, research, or beta testing to provide feedback on our Platform and Services.
- Interact with us through other means, such as direct communications or community programs.

  Additionally, this Privacy Notice applies whenever we provide a direct link to it, indicating that the terms set out herein govern the respective data processing activities.

This Privacy Notice does **not** apply to:

- External platforms, integrations, or third-party tools linked to our Platform. We do not control their data processing practices and recommend reviewing their privacy policies separately.
- When customers use our Platform to process personal data for their own business purposes, we act as a Data Processor and follow their instructions.
- Specific sites operated by Archiki that have their own Privacy Notice, which governs data processing. Please check the footer or legal sections of such sites.
- Personal data collected in connection with employment, contractor relationships, or job applications, which are subject to separate privacy notices.

### Contact Information

If you have any questions about this Privacy Notice or how we handle your data, you can contact us at info@archiki.com

**Archiki OÜ**

Address: Estonia, Harju maakond, Tallinn, Kesklinna linnaosa, Narva mnt 7-636, 10117

Registration Number: 17067356

Email: info@archiki.com

### Roles in Data Processing

We act as a Data Controller, determining the purposes and means of processing your personal data.

We may act in different capacities depending on the specific context of the data processing:

**As a Data Controller.** As a Data Controller, we determine the purposes and means of processing personal data in various contexts. In these cases, we are fully responsible for the collection and use of personal data, and this Privacy Notice governs all such processing activities.

**As a Data Processor.** In some cases, we act as a Data Processor, processing personal data on behalf of customers using our Platform. The customer, as Data Controller, determines the purposes and scope of processing, and we follow their instructions. This Privacy Notice does not apply to data controlled by customers. For any rights related to this data, please contact the relevant customer.

## Personal Data We Collect

The data we collect varies based on your interactions with us, including the features you use, the content you engage with, and the integrations you choose.

We collect personal data from the following sources:

- **Data You Provide** – Information you submit during registration, profile management, transactions, or communication with us.
- **Data Collected Automatically** – Technical, behavioral, and transactional data collected through system logs, cookies, tracking mechanisms, analytics tools, and security monitoring tools.
- **Data Received from Third Parties** – Information shared by integrated business tools, compliance partners, payment providers, logistics services, marketing partners, and other relevant third parties.

### Personal Data You Provide

We collect information you provide directly to us when using our Platform and its Services or engaging with us in other ways.

| Category | Details |
|---|---|
| Account and Profile Information | ■ Full name, email address, phone number;<br>■ Profile picture (if uploaded), bio, company role, username;<br>■ Date of birth, gender;<br>■ Social media handles (if provided). |

| | |
|---|---|
| Business and Professional Information | ■ Job title, role, company name;<br>■ Professional profiles, portfolios;<br>■ Professional qualifications, certifications, accreditations, or licenses (if provided). |
| Transaction and Financial Data | ■ Billing and shipping details, addresses;<br>■ Payment method, credit card details, bank account information;<br>■ Purchases, invoices, escrow transactions, financial settlements;<br>■ Tax identification number, financial documents (if required for regulatory compliance).<br><br>*Note: Payment data processed by third-party payment processors is subject to their privacy policies and security standards. We do not have access to payment data.* |
| Collaboration and Communication Data | ■ Messages from conversations in CRM, chat tools, project spaces;<br>■ Files, documents, images, business reports, contracts (if shared);<br>■ Team roles, assigned tasks, project details and timelines;<br>■ Collaboration history, workflow activities, decision logs;<br>■ Emails, chat messages, tickets submitted to our support team. |
| Identity Verification and Compliance Data (if required) | ■ Passport, government-issued ID or other personal identity documents;<br>■ Registration certificates, proof of ownership;<br>■ KYC (Know Your Customer) verification, tax compliance records;<br>■ Any documents required for fraud prevention, risk assessments, or due diligence. |
| Preferences and Engagement Data | ■ Subscription tier, account settings;<br>■ Notification settings, alerts for orders, project updates;<br>■ Marketing preferences, opt-in/out status for newsletters and promotions;<br>■ Usage of AI-generated content, personalization settings. |

| | |
|---|---|
| Business Activity Data | ■ Order processing details, services requested, payments completed;<br>■ Escrow transactions (payment holds, contract fulfillment approvals);<br>■ Agreement approvals, document interactions;<br>■ Project and procurement history, items ordered, delivery records. |
| Logistics and Supply Chain Data | ■ Order status, estimated delivery timelines.<br>■ Transport routes, real-time cargo updates.<br>■ Stock availability, supplier interactions. |
| Support and Customer Service Interactions | ■ Details of inquiries, reported issues, and support tickets;<br>■ Emails, chat logs, phone call records;<br>■ Device details, error logs, resolution steps (if required for technical troubleshooting). |
| Event and Survey Participation Data | ■ Name, contact details, company affiliation, event preferences;<br>■ Feedback, opinions, and other data submitted voluntarily;<br>■ Opt-in preferences for follow-ups, post-event marketing, and related communications. |
| Office Visit Data | ■ Name, contact details, company affiliation;<br>■ Date, time, and purpose of visit;<br>■ CCTV footage (if applicable), access control logs. |

**Personal Data Collected Automatically**

When you access and use the Website or Platform, certain data is collected automatically to ensure functionality, security, and analytics-driven improvements. The amount of data collected depends on the type of device you use and its settings.

| **Category** | **Details** |
|---|---|
| Technical and Device Data | ■ IP address, ISP (Internet Service Provider);<br>■ Device type, operating system, system language;<br>■ Browser type, version, extensions affecting platform functionality;<br>■ Unique device identifiers;<br>■ Screen resolution, UI/UX preferences. |

| | |
|---|---|
| Usage and Behavioral Data | ■ Login timestamps, session duration;<br>■ Pages viewed, clicks, time spent on different sections;<br>■ Use of specific tools and integrations;<br>■ AI-generated recommendations, workflow patterns. |
| Cookies and Tracking Technologies | Essential Cookies for basic functionality, such as secure logins and maintaining user sessions. |

**Data Received from Third-Party Services**

Archiki integrates with external platforms, service providers, and compliance partners who may share data to enhance security, financial operations, and business intelligence. We also receive information from other users, social media platforms, public databases, and business partners. This data may be combined with information collected through other means.

| **Category** | **Details** |
|---|---|
| Publicly Available Data | ■ Engagement with our official social media pages and groups;<br>■ Contact details from industry databases, professional networking platforms, and trade associations;<br>■ Business registration details, legal filings.<br>*We process this data in accordance with the respective platform's privacy policies and settings.* |
| Business Integrations and CRM Data | ■ Sales history, purchase patterns;<br>■ Engagement insights from CRM integrations;<br>■ Support tickets, chat logs, feedback. |
| Financial and Payment Services Data | ■ Payment processing status, fraud detection;<br>■ Invoice records, reconciliation data;<br>■ Information for tax regulatory reporting. |
| E-Signature and Document Management Data | ■ Signed agreements, timestamps, approval logs;<br>■ Compliance with document-signing requirements. |

| | |
|---|---|
| Logistics and Supply Chain Data | ■ Name, contact details of recipients or handlers;<br>■ Delivery addresses, delivery times, and tracking information;<br>■ Logistics provider details, including personnel involved in handling deliveries or shipments. |
| KYC and Compliance Data | ■ Identity authentication reports;<br>■ Anti-money laundering (AML) checks (if applicable). |
| Contact and Outreach Data | ■ Business contact details obtained from trusted providers;<br>■ Additional professional information linked to business interactions;<br>■ Data sourced through public or authorized third-party services for marketing and outreach purposes. |
| Marketing and Analytics Data | ■ Metrics on user interaction;<br>■ Insights from analytics tools;<br>■ Personalized ads based on user interests and behavior. |

### Purposes and Legal Bases for Processing

We process personal data for various business, operational, and legal purposes in compliance with applicable data protection laws.

The legal basis for processing depends on the nature of the data, the processing activity, and regulatory requirements.

- **Performance of a Contract.** We process personal data to fulfill our contractual obligations. Without this processing, we cannot deliver the requested services.
- **Legitimate Interests.** We process personal data based on our legitimate business interests (e.g., security, marketing, and service improvements), provided these interests do not override users' fundamental rights and freedoms. Users may object to such processing where applicable.
- **Legal Obligation.** Certain processing is required to comply with legal obligations, such as financial reporting and tax compliance.
- **Consent.** We obtain explicit consent before processing personal data, such as for direct marketing, non-essential cookies, sensitive data processing, and conducting surveys. You may withdraw your consent at any time, without affecting the lawfulness of processing prior to the withdrawal.

The table below outlines the purposes for processing, how personal data is used, and the applicable legal bases.

| Processing Purpose | Details | Legal Basis |
|---|---|---|
| Platform Functionality and Account Management | ■ Creating and managing user accounts, business profiles, and team access.<br>■ Providing access to core Platform features and Services.<br>■ Storing user-generated content (e.g., files, business documents, project data).<br>■ Enabling team collaborations and workflow automation.<br>■ Verifying login credentials, multi-factor authentication (MFA), and security authentication. | Performance of a Contract – Processing is necessary to provide Platform functionalities as per our Terms of Use.<br><br>Legitimate Interests – Ensuring usability, security, and efficiency of the Platform without overriding users' rights. |
| Payment Processing and Financial Transactions | ■ Facilitating secure transactions, including purchases, subscriptions, refunds, and escrow payments.<br>■ Processing invoices, billing details, and tax-related documentation.<br>■ Verifying financial details, such as payment methods and transaction history.<br>■ Preventing fraudulent transactions and enforcing financial security measures. | Performance of a Contract – Essential for executing transactions and financial agreements.<br><br>Legal Obligation – Compliance with tax laws, anti-fraud regulations, and financial reporting requirements. |
| Communications and Customer Support | ■ Sending account-related notifications, including confirmations, system updates, and service changes.<br>■ Facilitating in-app messaging, chat functions, project collaboration tools, and CRM functionalities. | Performance of a Contract – Necessary for essential service-related communications.<br><br>Legitimate Interests – Ensuring customer support and operational efficiency. |

| | | |
|---|---|---|
| | ■ Providing customer support via email, live chat, and helpdesk tickets.<br>■ Responding to inquiries, resolving technical issues, and assisting with troubleshooting. | Consent – Required for non-essential interactions, such as feedback requests. |
| Marketing, Advertising and User Engagement | ■ Sending newsletters, promotional emails, and product updates (where permitted).<br>■ Personalizing marketing campaigns, retargeting ads, and social media engagement.<br>■ Analyzing user engagement, ad performance, and behavioral trends.<br>■ Facilitating referral programs, surveys, giveaways, and loyalty rewards. | Consent – Required before sending direct marketing communications.<br><br>Legitimate Interests – Supporting business growth and user engagement, with an option to opt out. |
| Analytics, Platform Improvements and Feature Development | ■ Tracking usage patterns, preferences, user behaviour, and business activity to optimize services.<br>■ Conducting behavioral analytics and gathering user insights.<br>■ Improving platform features, testing new functionalities (Beta versions), and collecting user feedback.<br>■ Enhancing AI-driven recommendations, automated tools and predictive analytics for user experience improvements. | Legitimate Interests – Continuous Platform enhancement and user experience improvements.<br><br>Consent – Required where profiling or behavioral analysis involves personal data. |

| | | |
|---|---|---|
| Security, Fraud Prevention and Compliance | ■ Detecting, preventing, and investigating fraudulent activities, unauthorized access, and cybersecurity threats.<br>■ Verifying user identities for Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance.<br>■ Enforcing compliance with our Terms of Use, contractual obligations, legal requirements, and policies.<br>■ Complying with regulatory obligations, responding to law enforcement requests, and fulfilling law enforcement inquiries. | Legal Obligation – Compliance with cybersecurity, financial, and consumer protection laws.<br><br>Legitimate Interests – Maintaining security, preventing abuse, and safeguarding business operations. |
| Business Operations and Strategic Development | ■ Managing partnerships, business negotiations, and corporate transactions.<br>■ Conducting internal audits, performance evaluations, and operational analytics.<br>■ Expanding market reach, onboarding new users, and developing business strategies.<br>■ Processing professional contact details obtained from third-party services and business directories. | Legitimate Interests – Supporting business growth, partnerships, and strategic planning.<br><br>Consent – Required when using third-party data sources for marketing outreach. |

| | | |
|---|---|---|
| Event and Survey Participation | ■ Registering attendees for industry events, webinars, and business conferences.<br>■ Conducting user research, satisfaction surveys, and feedback analysis.<br>■ Sending follow-up communications and marketing content (where permitted). | Performance of a Contract – Where participation involves a contractual commitment.<br><br>Legitimate Interests – Business engagement and event organization.<br><br>Consent – Required for follow-up marketing communications. |
| Office Visits and Facility Security | ■ Registering visitors and managing office entry logs.<br>■ Enforcing physical security policies, such as access control systems.<br>■ Monitoring CCTV footage for security purposes (where applicable). | Legitimate Interests – Ensuring workplace security and facility management.<br><br>Legal Obligation – Compliance with local security regulations, where required. |

### Disclosure of Personal Data

We disclose personal and business-related information in accordance with legal obligations, contractual commitments, and operational requirements, while ensuring compliance with data protection laws. Archiki does not sell or rent personal data. However, we may share it under the circumstances outlined below, always in compliance with applicable data protection regulations.

**Other Platform Participants.** Certain interactions on the Platform involve controlled sharing of information to facilitate transactions, collaborations, and service engagements.

| Category | Details | Your Control |
|---|---|---|
| Contracting and Transactions | Relevant details may be disclosed to counterparties for contract negotiations, agreements, and payments. | Transaction visibility can be managed through platform settings; however, some disclosures are essential for contract execution. |

| | | |
|---|---|---|
| Project Collaboration and Workspaces | Information such as roles, uploaded documents, and project status may be visible to other authorized participants in shared workspaces or projects. | Access is managed through permissions and role-based controls. |
| Managed Accounts and Administrators | Organization administrators may access and manage your profile, activity logs, and business interactions within managed enterprise accounts. | Review your organization's administrator access policies. |
| Marketplace and Listings | Product listings, service offerings, or company profiles in the marketplace may be visible to potential buyers, suppliers, or partners, and could be indexed by search engines. | Visibility settings for marketplace content and profiles can be adjusted. |

**Service Providers and External Partners.** We work with third-party service providers to support Platform functionality, operational efficiency, and compliance, all under contractual agreements and in accordance with data protection regulations.

| Category | Details |
|---|---|
| Core Infrastructure and IT Services | Secure storage, processing, and transmission of data via cloud providers, server infrastructure, and security monitoring. |
| Payments, Finance and Compliance | Processing transactions, regulatory reporting, and tax compliance through financial entities and payment processors. |
| Verification, Compliance and Risk Management | Identity verification, fraud prevention, and regulatory compliance (KYC/AML) via specialized providers and legal advisors. |
| Business Operations and Advisory Services | Legal, marketing, and strategic support through external advisors, consultants, and contracted specialists. |

**Legal and Compliance.** We may disclose personal and business data when required to meet legal, regulatory, and security obligations.

| Category | Details | Your Control |
|---|---|---|
| Regulatory Compliance and Tax Obligations | Disclosures to government agencies or regulatory bodies for legal, tax, and financial reporting purposes. | Users may be notified when applicable. |

| | | |
|---|---|---|
| Law Enforcement and Government | Responses to lawful requests such as subpoenas, court orders, or regulatory investigations. | |
| Business Disputes and Contract Enforcement | Data sharing with legal representatives, arbitration bodies, or regulatory agencies for dispute resolution, fraud prevention, or compliance enforcement. | |
| Business Transactions and Corporate Changes | Data transfers in case of mergers, acquisitions, corporate restructuring, or asset transfers. | |

**Public Interactions.** If you engage with Archiki on social media, industry forums, or public channels, please be aware that:

| Category | Details | Your Control |
|---|---|---|
| Social Media Interactions | Your interactions on our official social media pages may be visible to others. | Users can manage their privacy settings where applicable. |
| Public Business Profiles | Listings and profiles may be indexed by search engines. | |
| Success Stories and Testimonials | Archiki may highlight case studies with prior consent. | Users provide consent before inclusion. |

**User-Controlled Disclosures.** Users may choose to share information voluntarily through various Platform features.

| Category | Details | Your Control |
|---|---|---|
| Business Networking Features | Sharing company profiles with potential partners, suppliers, or buyers. | Users can control visibility settings where applicable. |
| Public Product Catalogs and Listings | Making product offerings visible to external buyers. | |
| Community Discussions and Forums | Participating in industry forums, knowledge-sharing spaces, or business communities. | Users should be aware that discussions may be publicly accessible. |

Any information you share outside of our privacy settings is at your discretion. Archiki is not responsible for how others or third parties handle publicly disclosed information.

**Disclosures of Aggregated or Anonymized Data**

We may share non-identifiable and aggregated data for analytical and business purposes, such as:

| Category | Details |
|---|---|
| Research and Insights | Analysis of general usage trends without identifying individuals or businesses. |
| Performance Benchmarking | Operational analytics for service improvement. |
| Product Development | Enhancing automated recommendations and refining platform features. |

### Data Storage and Security Measures

We have implemented technical and organizational measures to ensure your data remains secure and to provide you with a safe experience.

Your data is securely stored on servers within the European Economic Area (EEA) and with trusted cloud providers who meet international security standards. These providers are contractually obligated to safeguard your data.

We use industry-standard security measures, including encryption and access controls, to protect your data during transmission and storage. Regular internal audits help identify and address potential vulnerabilities in our systems.

While we implement strong security measures, no system can guarantee absolute security, and risks may persist during data transmission and storage. However, we are committed to continually improving our security practices to minimize these risks.

You also play a role in securing your data. We recommend using strong passwords and enabling multi-factor authentication (MFA) for added protection. Please keep your login credentials confidential and avoid sharing them with others.

### Data Retention and Management

We retain personal data based on the type of data and the purpose for which it was collected. After the retention period expires, we securely delete, anonymize, or archive the data.

We retain personal data only for as long as necessary to fulfill the purposes outlined in this Privacy Notice or as required by applicable laws. Retention periods are determined based on the nature of the data, legal and regulatory obligations, contractual requirements, business needs, and security considerations. Once data is no longer needed, we securely delete, anonymize, or archive it in accordance with our data management practices.

**Retention of Specific Data Categories**

- **User Account Information.** Retained as long as your account remains active. If you terminate your account, certain data may be retained temporarily to comply with legal requirements before being deleted or anonymized.
- **Customer Support and Communication Data.** Retained for as long as necessary to address issues, improve services, or ensure ongoing support.
- **Analytics and Behavioral Data.** Retained for the duration necessary to enhance the Platform's functionality and improve the user experience.
- **Marketing Data.** Retained until you opt out or unsubscribe. Post-unsubscribing, data may be retained briefly to ensure compliance with your preferences and prevent further communication.
- **Project and Collaborative Data.** Retained for the duration of the project. After completion, data is kept as needed for reporting and analysis.
- **Contractual Data.** Retained for the length of the contractual relationship and any required period following termination to address any issues, including disputes, invoices, or transaction histories.
- **Security and Fraud Prevention Data.** Retained as needed due to compliance obligations or to manage disputes.
- **Third-Party Integrations.** Retained in accordance with the privacy policies of the third-party providers.

In some cases, we may be required by law to retain data for longer periods, such as for legal proceedings, disputes, or regulatory compliance. After the retention period ends, data will be securely archived, and upon expiration or request, we will delete or anonymize it using industry-standard methods. If deletion is not immediately possible (e.g., for legal reasons), the data will be securely archived and made inaccessible for any other purposes.

For more information on managing your data and exercising your rights, please refer to the "Your Privacy Rights" section.

### International Transfers

Archiki may transfer, store, and process your personal data outside your country of residence, in compliance with applicable data protection laws and security measures.

International transfers may occur in the following contexts:

- Third-party service providers supporting operations, infrastructure, analytics, marketing, and customer support.
- Business partners and affiliates assisting in service delivery and platform functionality.
- Internal corporate transfers within our group entities.

We conduct regular security assessments of third-party data recipients and impose contractual obligations to ensure compliance with security standards and data protection laws, including measures like encryption, pseudonymization, and anonymization to protect your data.

For transfers of personal data to countries without an adequacy decision, we rely on one or more of the following legal mechanisms:

- **Standard Contractual Clauses (SCCs).** For transfers outside the EEA, UK, or Switzerland to countries lacking an adequacy decision, we use SCCs approved by the European Commission or the UK's ICO to ensure a legally recognized level of protection.
- **EU-U.S. Data Privacy Framework (DPF).** Where applicable, we transfer data to U.S.-based service providers certified under the EU-U.S. Data Privacy Framework (DPF), the UK Extension, and the Swiss-U.S. DPF, ensuring compliance with strict data protection standards.
- **Binding Corporate Rules (BCRs).** When transferring data within our corporate group, we may implement BCRs to ensure consistent data protection across our global operations.
- **Other Legally Recognized Mechanisms.** Where SCCs, adequacy decisions, or BCRs do not apply, we may rely on additional legal bases, such as explicit user consent or transfers necessary for contract performance, in accordance with applicable data protection laws.

### Your Privacy Rights

You have rights regarding your personal data, including the ability to access, correct, delete, or restrict its processing.

Depending on your location and applicable data protection laws, you may have the following rights regarding your personal data:

- **Right to Access.** You may request confirmation of whether we process your personal data. If we do, you can obtain a copy along with details on the categories of data processed, purposes, recipients, data sources (if not collected directly from you), and other relevant to the processing information.
- **Right to Rectification**. If your personal data is inaccurate or incomplete, you can request corrections. Certain updates, such as name or contact details, can be made directly in your account settings. For other corrections, contact us.

- **Right to Erasure ("Right to be Forgotten").** You may request deletion of your personal data in specific cases, such as when it is no longer necessary, you withdraw consent, you object to processing, or the data has been unlawfully processed. However, legal, regulatory, or contractual obligations may require us to retain certain data. If full erasure is not possible, we will inform you of the reason.
- **Right to Restriction of Processing.** You may request that we restrict processing under specific circumstances, including when you contest the accuracy of the data, processing is unlawful but you prefer restriction over deletion, or you require the data for legal claims. While restricted, we may store the data but will not actively process it unless legally required.
- **Right to Data Portability.** If processing is based on your consent or contract performance, you may request a structured, commonly used, and machine-readable copy of your personal data. Some data can be exported via Platform settings. For other formats or direct transfers, contact us.
- **Right to Object to Processing.** You may object to the processing of your personal data, including when it is used for direct marketing, automated profiling, or based on legitimate interests, unless we can demonstrate overriding legal grounds for continued processing.
- **Right to Withdraw Consent.** If processing is based on consent (e.g., marketing preferences), you may withdraw consent at any time without affecting prior lawful processing.
- **Rights Related to Automated Decision-Making.** If we make decisions that significantly affect you solely through automated processes, we will inform you if such processing occurs and, where required, provide the opportunity to request human intervention, express your viewpoint, or contest the decision.
- **Right to Lodge a Complaint.** If you believe your data protection rights have been violated, you may file a complaint with the relevant supervisory authority:

  For EEA Residents: Contact your local Data Protection Authority (DPA).

  For UK Residents: Contact the UK Information Commissioner's Office (ICO).

  For Other Jurisdictions: Refer to your national data protection authority.

**Exercising Your Privacy Rights**

We offer clear mechanisms for managing your privacy preferences and exercising your privacy rights.

**Submitting a Request.** You can exercise your rights by either using the self-service tools within your Archiki account or contacting us at info@archiki.com with your request details. To ensure a prompt response, please include:

- The specific right(s) you wish to exercise.
- Information sufficient to verify your identity (e.g., name, email, account details).

- Any relevant details necessary for processing your request.

We will process your request within the timeframe required by law and inform you if additional information is needed.

**Appealing a Decision.** If we are unable to fulfill your request or you are dissatisfied with our response, you may appeal the decision by contacting us at info@archiki.com. We will conduct a fair and transparent review of your appeal.

**Verification Process.** To protect your privacy and prevent unauthorized access, we may need to verify your identity before processing your request. The verification requirements will vary based on the type of request and applicable laws and may include providing identifying information such as your name, email address, or account details, submitting supporting documents when necessary, or confirming your residency to comply with jurisdiction-specific regulations. If we are unable to verify your identity, or if fulfilling the request would compromise another person's privacy or conflict with legal obligations, we may not be able to proceed with your request.

**Authorized Agents.** If you designate someone to act on your behalf, we require the following: a signed authorization letter or valid power of attorney, verification of both your identity and the agent's authority, and direct confirmation from you before we proceed with the request.

**Managing Your Privacy Preferences**

- **Updating Your Personal Data.** You can review and update your information through your account settings or by contacting us.
- **Deleting Your Account.** To permanently delete your Archiki account and associated data you can submit a request through the Platform or contact us at info@archiki.com. We will process your request as per legal retention policies.
- **Managing Marketing Communications.** You can opt out of marketing communications by using the "unsubscribe" link in emails, adjusting preferences in your account settings or contacting us directly. Please note, even after opting out, you may continue to receive essential service-related communications (e.g., account notifications, security alerts).
- **Managing Linked Third-Party Services.** If you have connected your Archiki account to third-party services, you can manage or disconnect them through the relevant service settings.
- **Sending "Do Not Track" (DNT) Signals.** Some browsers allow you to send Do Not Track (DNT) signals. While we provide privacy controls such as cookie settings and ad opt-outs, we may not be able to respond to all DNT signals due to industry standards.
- **Exporting Your Data.** You can export your data directly through the Platform's settings. If additional assistance is required, please contact us.

## Changes to this Privacy Notice

We may update this Privacy Notice from time to time to reflect changes in legal requirements or regulatory developments, updates to our business practices or Service functionalities, or improvements to our privacy and security measures.

If we make material changes, we will notify you through appropriate channels, such as email notifications, in-app alerts, or website banners, where required by law.

## Children's Privacy

Our Platform, Website, and Services are not directed at individuals under the age of 18 (or the applicable age of majority in their jurisdiction). We do not knowingly collect, process, or store personal data from children without verified parental consent.

If we become aware that we have inadvertently collected data from a child without proper consent, we will take immediate steps to delete it.

If you are a parent or legal guardian and believe that your child has provided us with personal data, you may contact us at info@archiki.com to request its deletion.

## Third-Party Services and Integrations

We integrate with third-party services to enhance our Platform and its Services, including payment processors, analytics providers, cloud storage services, and other business tools and integrations

These third-party services operate independently, and their use of personal data is governed by their own privacy policies. We do not control how third parties process your data and encourage you to review their privacy policies before engaging with them.

Additionally, our Platform and Websites may contain links to external websites, social media platforms, or third-party services. If you interact with these external services, your data may be subject to their privacy practices, which are beyond our control. We disclaim any responsibility for the privacy policies or practices of third parties.

## Additional Disclosures for U.S. Residents

This section supplements our Privacy Notice and applies exclusively to residents of the United States. It outlines your rights under applicable state privacy laws and explains how Archiki collects, processes, and discloses personal data in compliance with these laws.

For further details, please refer to:

- **"Personal Data We Collect"** – Information about the categories of personal data we collect.

- **“Purposes and Legal Bases for Processing”** – Explanation of why and how we process your personal data.
- **“Disclosure of Personal Data”** – Information on how and with whom we share personal data.
- **“Data Retention and Management”** and **“Data Storage and Security Measures”** – Details on how long we retain your data and the security measures we apply.
- **“Your Privacy Rights”** – A breakdown of your privacy rights and how to exercise them.

**Your Privacy Rights Under U.S. State Laws**

If you reside in certain U.S. states, you may have specific rights regarding your Personal Information under applicable state privacy laws. These rights vary by state and may include the following:

- **Right to Know / Access.** You have the right to request information about:
  - The categories of personal information we collect.
  - The sources from which we collect your personal information.
  - The purposes for which we use your personal information.
  - The categories of third parties with whom we share your information.
  - Specific pieces of personal information we hold about you.
- **Right to Delete.** You can request the deletion of your personal information, subject to certain legal or regulatory exceptions.
- **Right to Correct.** If your personal information is inaccurate or outdated, you have the right to request corrections.
- **Right to Opt-Out of Targeted Advertising, Sales, and Profiling.** Some U.S. state laws classify sharing data for targeted advertising as a “sale” of personal information. You have the right to:
  - Opt out of the sale or sharing of your personal data for targeted advertising.
  - Opt out of profiling when it is used to make significant decisions about you.
  - Limit the use of tracking technologies that facilitate personalized ads.

  Archiki does not sell personal information. However, we may disclose or share data in accordance with this Privacy Notice for legitimate business purposes, compliance obligations, or to improve and personalize your experience on the Platform.

  **How to Opt-Out:** You can exercise these rights by contacting us at info@archiki.com.
- **Right to Limit the Use of Sensitive Personal Information.** If we process sensitive personal information, you may restrict its use to only what is necessary for providing our services.

- **Right to Data Portability.** You may request your personal data in a structured, machine-readable format.
- **Right to Non-Discrimination.** Exercising your privacy rights will not result in denial of services, different pricing or service levels, or any form of retaliation.
- **Right to Authorize an Agent.** You may designate an authorized agent to submit privacy-related requests on your behalf by providing written authorization.

For details on how to exercise your rights, please refer to the **"Exercising Your Privacy Rights"** section.

### Notice for California Residents

Archiki collects, processes, and shares personal information in connection with our Platform and its Services, in compliance with the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA).

The table below provides an overview of:

- Categories of personal information we collect.
- Purposes for which we process this information.
- Third parties with whom we disclose data for business purposes.
- Third parties with whom we share data for targeted advertising.

**Categories of Personal Information Collected and Shared**

| Category of Personal Information We Collect | Purposes for Collection & Disclosing | Third Parties to Whom We Disclose for Business Purposes |
|---|---|---|
| **Identifiers**<br>Name, email, phone number, IP address, unique account identifiers. | ▪ Providing and managing access to Archiki's Platform and its Services.<br>▪ Verifying user identity and securing accounts.<br>▪ Facilitating customer support and communications.<br>▪ Personalizing user experience.<br>▪ Ensuring compliance with legal obligations. | ▪ Service providers (e.g., hosting, authentication, customer support).<br>▪ Payment processors.<br>▪ Legal and professional advisors.<br>▪ Government authorities (where required by law). |

| | | |
|---|---|---|
| **Commercial Information**<br>Subscription details, transaction history, service usage records. | ▪ Processing transactions and payments.<br>▪ Managing billing and account services.<br>▪ Conducting analytics to improve our business. | ▪ Payment processors.<br>▪ Logistics and fulfillment providers.<br>▪ Legal and financial advisors. |
| **Internet or Network Activity**<br>Browsing history on Archiki's Platforms and Websites, session data, log data, cookies, interactions with the Platform. | ▪ Improving functionality.<br>▪ Detecting and preventing fraud or security threats.<br>▪ Conducting analytics for service enhancement. | ▪ Cybersecurity and fraud prevention services.<br>▪ Analytics providers. |
| **Geolocation Data**<br>Approximate location based on IP address or device settings. | ▪ Enhancing security and fraud detection.<br>▪ Adapting services based on regional availability. | ▪ Security and fraud prevention partners. |
| **Employment and Business Information**<br>Company name, job title, industry, business affiliations. | ▪ Verifying business accounts.<br>▪ Facilitating sales and business interactions. | ▪ Business partners.<br>▪ CRM and procurement integrations. |
| **Sensory Data**<br>Audio, electronic, or visual data (e.g., recorded customer support interactions). | ▪ Customer support and quality assurance.<br>▪ Security and compliance monitoring. | ▪ Service providers handling customer support tools. |
| **Inferences**<br>Preferences, behavioral insights, engagement history with Archiki. | ▪ Personalizing user experience.<br>▪ Improving platform functionality.<br>▪ Enhancing analytics and marketing strategies. | ▪ Analytics providers.<br>▪ Providers of Business Information. |