SPIRITT Privacy Policy

Effective Date: June 10, 2026

This Privacy Policy explains how SPIRITT, Inc. and its affiliates, including SPIRITT Labs Ltd., collect, use, disclose, store, and protect personal data when you use SPIRITT's websites, workspaces, AI agents, software tools, integrations, APIs, hosted artifacts, generated applications, and related services.

For purposes of this Privacy Policy, "SPIRITT," "we," "us," and "our" mean SPIRITT, Inc., a Delaware corporation, and its affiliates, including SPIRITT Labs Ltd., unless a separate written agreement identifies a different entity.

This Privacy Policy does not replace any separate data processing agreement, enterprise agreement, or written agreement between SPIRITT and a customer. If a separate written agreement applies and conflicts with this Privacy Policy, that agreement controls for the covered customer data.

1. Overview

SPIRITT provides an AI native workspace and automation platform that helps users create, operate, deploy, automate, improve, and manage software, workflows, digital assets, and business operations.

The Service may process prompts, files, code, documents, credentials, application data, connected account data, agent logs, workflow activity, generated outputs, and other information needed to provide the Service.

Depending on the context, SPIRITT may act as a controller, processor, service provider, or similar role under applicable privacy laws.

For personal data we process on behalf of business customers or their End Users, the customer is generally responsible for determining the purposes and means of processing, and SPIRITT processes such data according to the customer's instructions and applicable agreements.

2. Data We Collect

SPIRITT may collect the categories of data described below depending on how you use the Service.

3. Account Data

We may collect name, email address, phone number, company name, role, login identifiers, authentication details, workspace membership, account settings, subscription information, and related account administration data.

We use Account Data to create and administer accounts, authenticate users, provide access to the Service, manage workspaces, provide support, communicate with users, enforce terms, prevent abuse, and comply with law.

4. Payment and Billing Data

We may collect billing information, subscription plan information, invoices, transaction records, payment status, tax information, and partial payment card details.

Payments are processed by payment providers such as Stripe. SPIRITT generally does not store full payment card numbers.

We use Payment and Billing Data to process payments, manage subscriptions, prevent fraud, maintain financial records, comply with tax and accounting obligations, and resolve billing issues.

5. Inputs, Outputs, Workspace Data, and Artifacts

We may collect prompts, instructions, uploaded files, documents, code, application data, project data, generated outputs, messages, automations, browser actions, agent logs, deployment data, workflow data, connected repository data, tool results, and data from services you connect.

We use this data to provide the Service, generate Outputs, operate agents, build and maintain Artifacts, debug issues, deploy software, execute workflows, provide support, secure the Service, and improve SPIRITT's products, services, AI systems, evaluations, workflows, and safety systems.

6. Connected Service Data

If you connect third party services, SPIRITT may collect and process data from those services according to the permissions you grant, your instructions, and the functionality you use.

Connected Service Data may include data from identity providers, developer platforms, cloud services, communication tools, analytics tools, customer systems, payment providers, Google services, Meta services, repositories, databases, browsers, and other applications or APIs.

The exact data depends on the integration, permissions, scopes, account settings, third party platform, and actions you request.

We use Connected Service Data to authenticate users, perform requested actions, retrieve information, update records, send communications, deploy applications, analyze data, operate workflows, provide support, secure the Service, and improve the Service where permitted.

7. Google OAuth Data

If you connect Google services, SPIRITT may access Google user data only according to the OAuth scopes and permissions you approve.

Depending on the permissions granted, this may include basic profile information, email address, files, file metadata, calendar data, communication data, workspace data, cloud data, or other Google API data you authorize.

SPIRITT's use and transfer of information received from Google APIs will comply with the Google API Services User Data Policy, including Limited Use requirements where applicable.

SPIRITT uses Google user data only to provide or improve user facing features, authenticate users, execute actions requested by users, maintain security, prevent abuse, comply with law, provide support where permitted, and perform internal operations using aggregated or de identified data where allowed.

SPIRITT does not sell Google user data, use Google user data for unrelated advertising, transfer Google user data to data brokers, or use Google user data to determine creditworthiness.

Human access to Google user data is limited as required by Google policy, including where you give affirmative permission, where necessary for security, where necessary for legal compliance, or for internal operations using aggregated data where allowed.

8. Meta Platform Data

If you connect Meta services, SPIRITT may access Meta Platform Data according to the permissions you approve.

Depending on the permissions granted, this may include profile data, email address, page or business information, ad account data, insights, analytics, messaging related data, access tokens, identifiers, or other Meta data you authorize.

SPIRITT processes Meta Platform Data only as described in this Privacy Policy, as permitted by the permissions you grant, and as required by applicable Meta platform policies.

SPIRITT may use Meta data to authenticate users, provide connected Meta features, access assets you authorize, retrieve analytics or account data you request, execute actions you authorize, secure and maintain the Service, prevent abuse, and comply with law.

SPIRITT does not sell Meta Platform Data or process it for undisclosed purposes.

Users may request deletion of Meta related data by contacting info@spiritt.io.

9. Technical and Usage Data

We may collect IP address, device identifiers, browser type, operating system, referring pages, pages viewed, session activity, feature usage, logs, error reports, performance data, approximate location, cookie data, and similar technical information.

We use Technical and Usage Data to operate the Service, secure accounts, detect abuse, analyze performance, improve reliability, debug issues, understand usage, personalize experiences, support users, enforce terms, and comply with law.

10. Communications and Support Data

If you contact SPIRITT, we may collect your contact details and the content of your messages, support requests, call notes, attachments, feedback, and related metadata.

We use this data to respond to you, provide support, troubleshoot issues, improve the Service, train support processes, maintain records, and protect our rights.

11. Feedback, Ratings, and Research Data

We may collect feedback, ratings, corrections, bug reports, surveys, interviews, research participation data, and other materials you provide.

We may use this data to improve SPIRITT’s products, services, AI systems, evaluations, workflows, and safety systems.

12. End User Data

If you use SPIRITT to operate applications, automations, websites, agents, workflows, or services for End Users, SPIRITT may process End User data on your behalf.

End User data may include data submitted by End Users, data collected through Artifacts, communications, transaction data, usage data, files, identifiers, and other information determined by your configuration and use of the Service.

You are responsible for providing required notices, obtaining required consents, maintaining required legal bases, honoring End User rights, and complying with applicable privacy, consumer protection, and data protection laws.

If you are an End User of a SPIRITT customer, please contact that customer first regarding privacy requests.

13. Data from Cookies and Similar Technologies

SPIRITT may use cookies, pixels, local storage, software development kits, and similar technologies.

These technologies may help keep users signed in, remember preferences, secure accounts, measure usage, understand performance, detect fraud, provide support, personalize experiences, and measure marketing effectiveness.

You can control cookies through browser settings and consent tools where available. Some features may not work properly without certain cookies.

14. How We Use Data

SPIRITT may use data to:

1. provide, operate, maintain, and secure the Service;
2. create and administer accounts;
3. authenticate users;
4. process payments;
5. generate Outputs;
6. operate AI agents and automations;
7. access Connected Services at your direction;
8. build, debug, host, deploy, monitor, and maintain Artifacts;
9. provide support;
10. personalize the Service;
11. analyze usage and performance;
12. detect and fix errors;
13. prevent fraud, abuse, security incidents, and illegal activity;
14. enforce SPIRITT's Terms;
15. comply with law and legal process;
16. send service communications;
17. send marketing communications where permitted;
18. develop new features; and
19. improve SPIRITT's products, services, AI systems, evaluations, workflows, and safety systems.

15. Service Improvement and AI System Improvement

Unless restricted by a separate written agreement, supported account settings, applicable law, or provider specific policies, SPIRITT may use Inputs, Outputs, workspace activity, usage data, logs, feedback, Connected Service Data, and interaction data to improve SPIRITT's products, services, AI systems, evaluations, workflows, and safety systems.

This may include quality evaluation, product analytics, safety testing, abuse detection, debugging, workflow optimization, feature development, internal research, benchmarking, and evaluation.

SPIRITT may create and use aggregated, anonymized, or de identified data for analytics, research, security, product development, service improvement, and business purposes.

Your use of SPIRITT does not transfer ownership of your User Content or Outputs to SPIRITT.

16. Legal Bases for Processing

Where applicable law requires a legal basis, SPIRITT may process personal data based on one or more of the following:

1. performance of a contract, including providing the Service;
2. legitimate interests, including security, fraud prevention, service improvement, support, analytics, and business operations;
3. consent, including where you authorize integrations or marketing;
4. compliance with legal obligations;
5. protection of vital interests where necessary; and
6. establishment, exercise, or defense of legal claims.

Where processing is based on consent, you may withdraw consent where applicable, but withdrawal does not affect processing that occurred before withdrawal.

17. Human Access to User Data

Authorized SPIRITT personnel or contractors may access user data where reasonably necessary to provide support, debug or fix issues, improve the Service, investigate abuse or security incidents, comply with law, enforce terms, process feedback, or operate services you request.

Access is limited based on role, need, security controls, and operational requirements.

18. Service Providers

SPIRITT uses third party service providers to operate, secure, analyze, support, and improve the Service.

These providers may include payment processors, cloud infrastructure providers, AI model providers, analytics providers, communication providers, customer support providers, security providers, authentication providers, developer platforms, and Connected Service providers selected by you.

SPIRITT shares data with providers only as reasonably necessary to provide, secure, support, analyze, or improve the Service, comply with law, process payments, or perform actions you request.

SPIRITT may update service providers as the Service evolves.

19. AI Model Providers

SPIRITT may send Inputs, Outputs, files, code, prompts, logs, or other data to AI model providers to generate responses, operate agents, evaluate outputs, or provide requested functionality.

Provider specific data handling may vary by product, configuration, region, and account type. SPIRITT handles such processing according to applicable agreements, provider terms, user permissions, and applicable law.

20. Affiliates

SPIRITT affiliates may process data to provide, secure, support, and improve the Service.

SPIRITT Labs Ltd. may own or operate certain technology and intellectual property used to provide the Service.

SPIRITT may share data among affiliates where reasonably necessary for business operations, service delivery, support, security, compliance, and improvement.

21. Sharing Data

SPIRITT may share data:

1. with service providers;
2. with AI model providers;
3. with Connected Services at your direction;
4. with affiliates;
5. with your organization or administrator, if your account belongs to an organization;
6. with payment processors;
7. with analytics and marketing providers where permitted;
8. with legal, security, or compliance advisors;
9. with regulators, courts, or law enforcement where required or appropriate;
10. in connection with a merger, acquisition, financing, restructuring, bankruptcy, or sale of assets; and

11. with your consent or instruction.

SPIRITT does not sell your User Content.

22. Organization Accounts

If you use the Service through an organization, employer, customer, or team account, administrators may access, control, export, restrict, monitor, or delete your account, workspace, activity, User Content, Outputs, Artifacts, integrations, and settings.

Your organization may have its own policies governing use of the Service.

23. Connected Services and Third Party Websites

When you connect or use a Connected Service, SPIRITT may send data to that service and receive data from that service to perform actions you request.

Connected Services process data under their own terms and privacy policies. SPIRITT does not control and is not responsible for third party privacy or security practices.

Before connecting a service, you should review the relevant permissions, scopes, terms, and privacy policies.

24. Illegal Activity, Abuse, and Safety

SPIRITT may process, preserve, review, and disclose data where reasonably necessary to detect, prevent, investigate, stop, or respond to illegal activity, abuse, security incidents, fraud, policy violations, harm, or threats to the rights, safety, property, or security of SPIRITT, users, End Users, third parties, or the public.

SPIRITT may refuse, block, suspend, terminate, preserve, remove, disable, or report activity where SPIRITT believes the activity may be unlawful, unsafe, abusive, infringing, fraudulent, or non compliant.

25. Security

SPIRITT uses reasonable technical and organizational measures designed to protect data, including access controls, credential management, monitoring, encryption in transit where appropriate, security procedures, and operational safeguards.

No system is completely secure. You are responsible for protecting your account, credentials, devices, integrations, End User permissions, and backups.

You should notify SPIRITT promptly if you suspect unauthorized access or security issues.

26. Data Retention

SPIRITT retains data for as long as reasonably necessary to provide the Service, maintain accounts, support users, improve the Service, comply with legal obligations, resolve disputes, enforce agreements, maintain security, prevent abuse, keep backups, and meet tax, audit, and accounting requirements.

Retention periods may vary by data type, account type, provider, integration, legal requirement, user settings, and operational needs.

SPIRITT may retain aggregated, anonymized, or de identified data where permitted by law.

27. Deletion

You may request deletion of personal data by contacting info@spiritt.io.

For Connected Services such as Google or Meta, you may also disconnect the integration where available.

Some data may be retained where necessary for legal compliance, security, fraud prevention, dispute resolution, backups, audit records, enforcement of agreements, legitimate business purposes, or as otherwise permitted by law.

Deletion from active systems may not immediately delete copies from backups or logs, which are deleted or overwritten according to retention cycles.

28. Data Export and Portability

Where required by law or supported by the Service, you may request access to or export of certain personal data.

Export functionality may not include all logs, derived data, internal records, security records, model evaluation data, or SPIRITT Technology.

29. International Transfers

SPIRITT may process data in locations where SPIRITT and its affiliates, service providers, and infrastructure providers operate.

Where required, SPIRITT uses appropriate safeguards, such as adequacy decisions, standard contractual clauses, data processing agreements, or other lawful transfer mechanisms.

By using the Service, you understand that data may be processed outside your country of residence.

30. Privacy Rights

Depending on your location, you may have rights to access, correct, delete, restrict, object to, or port personal data, withdraw consent, opt out of certain marketing or targeted advertising, limit certain uses of sensitive personal data, or lodge a complaint with a supervisory authority.

To exercise rights, contact info@spiritt.io. SPIRITT may verify your identity before responding.

If you are an End User of a SPIRITT customer, please contact that customer first. SPIRITT may refer your request to the relevant customer where appropriate.

31. United States Privacy Disclosures

Certain United States privacy laws may provide rights to residents of specific states.

SPIRITT may collect identifiers, commercial information, internet or network activity, geolocation approximations, professional information, inferences, sensitive information you choose to provide, and other categories described in this Privacy Policy.

SPIRITT collects such information from you, your organization, your devices, your use of the Service, Connected Services, service providers, and third parties you authorize.

SPIRITT uses and discloses such information for the purposes described in this Privacy Policy.

SPIRITT does not sell your User Content. If SPIRITT engages in activities considered a “sale” or “sharing” of personal information under applicable law, SPIRITT will provide required notices and choices.

32. European Region, United Kingdom, and Similar Rights

If applicable law provides GDPR style rights, you may have rights to access, rectification, erasure, restriction,

portability, objection, and withdrawal of consent.

You may also have the right to complain to a supervisory authority.

SPIRITT may rely on contract, legitimate interests, consent, legal obligation, vital interests, or legal claims as legal bases for processing.

33. Israel Privacy Disclosures

Where Israeli privacy law applies, SPIRITT provides notice of the identity and contact details of the controller, processing purposes, rights to access and correction where applicable, and consequences of refusing to provide information where required.

Providing certain information may be necessary to use the Service. If you do not provide required information, SPIRITT may be unable to provide some or all of the Service.

Privacy questions may be sent to info@spiritt.io.

34. Marketing Communications

SPIRITT may use contact, usage, and analytics data to send product updates, newsletters, offers, and marketing communications where permitted.

You may opt out of marketing emails using the unsubscribe link or by contacting SPIRITT.

SPIRITT may still send service, security, legal, billing, and transactional messages.

35. Children

The Service is not directed to children under 18. SPIRITT does not knowingly collect personal data from children under 18.

If you believe a child provided personal data to SPIRITT, contact SPIRITT.

36. Automated Processing and AI

SPIRITT uses automated systems and AI systems to provide the Service, generate Outputs, operate agents, detect abuse, improve reliability, evaluate performance, and secure the Service.

Outputs may be inaccurate, incomplete, or unsuitable. Users are responsible for reviewing Outputs and ensuring lawful use.

SPIRITT does not intend the Service to be used as the sole basis for decisions that produce legal or similarly significant effects without appropriate human review and legal compliance.

37. Sensitive Data

You should not submit sensitive personal data, regulated health data, financial account data, government identifiers, children’s data, biometric data, payment card data, or other highly sensitive information unless your agreement with SPIRITT permits it and you have all required rights, consents, safeguards, and legal bases.

If you submit sensitive data, you are responsible for ensuring that the submission and processing comply with applicable law.

38. Enterprise and Customer Data

For business customers, a separate agreement, order form, Data Processing Agreement, or enterprise terms may apply.

If there is a conflict between this Privacy Policy and a signed agreement, the signed agreement controls for that customer.

Enterprise customers may have additional controls, settings, restrictions, retention terms, or data use commitments.

39. Changes to This Policy

SPIRITT may update this Privacy Policy from time to time.

If changes are material, SPIRITT will provide notice where required.

The updated policy will show the effective date. Continued use of the Service after an update means the updated policy applies to future use.

40. Contact

Questions or privacy requests may be sent to info@spiritt.io.

Schedule 1. Categories of Personal Data

Depending on your use of the Service, SPIRITT may process identifiers, contact details, account credentials, online identifiers, device identifiers, commercial information, billing information, internet or network activity, approximate location, professional information, communications content, files, documents, code, prompts, generated outputs, support messages, preferences, inferences, security logs, and other information you provide or authorize.

Some data may be considered sensitive under applicable laws if you choose to provide it, including credentials, precise content of communications, files containing sensitive information, authentication tokens, financial records, health related information, government identifiers, or other regulated information.

You should not provide sensitive data unless your agreement permits it and you have all required rights, notices, consents, and safeguards.

Schedule 2. Sources of Personal Data

SPIRITT may collect personal data from:

1. you;
2. your organization;
3. your devices and browsers;
4. your use of the Service;
5. Connected Services you authorize;
6. End Users who interact with your Artifacts;
7. service providers;
8. payment processors;
9. identity providers;
10. developer platforms;
11. security and fraud prevention providers;
12. analytics providers;
13. public sources where permitted; and
14. third parties you direct or authorize.

Schedule 3. Purposes of Processing

SPIRITT processes personal data for service delivery, authentication, account management, billing, support, communication, deployment, hosting, agent operation, automation, connected service access, security, fraud prevention, abuse detection, legal compliance, service improvement, AI system improvement, evaluation, debugging, analytics, research, and business operations.

SPIRITT may also process data to enforce terms, protect rights, respond to legal process, investigate incidents, prevent harm, and maintain trust and safety.

Schedule 4. Disclosure Categories

SPIRITT may disclose personal data to affiliates, service providers, AI model providers, payment processors, identity providers, Connected Services, analytics providers, communications providers, security providers, professional advisors, legal authorities, business transaction parties, and others with your consent or instruction.

SPIRITT may disclose different categories of data depending on the purpose. For example, payment providers receive billing data, AI model providers may receive Inputs and context needed to generate Outputs, Connected Services receive data needed to perform requested actions, and security providers may receive logs or identifiers needed to prevent abuse.

Schedule 5. AI Processing Details

SPIRITT uses AI systems to generate Outputs, operate agents, summarize information, write code, analyze files, classify content, identify errors, detect abuse, evaluate quality, route tasks, and improve user experience.

AI systems may process Inputs, Outputs, files, prompts, code, logs, metadata, and Connected Service data where necessary for requested functionality.

AI Outputs may contain personal data if Inputs contain personal data or if the task requires processing personal data.

SPIRITT may use automated systems to detect policy violations, security risks, abuse, fraud, operational issues, or unsafe behavior.

SPIRITT does not intend users to rely on AI Outputs as the sole basis for decisions that have legal or similarly significant effects without appropriate human review.

Schedule 6. Agent and Automation Data

Agents and automations may access workspace data, files, repositories, browsers, APIs, credentials, Connected Services, messages, calendars, documents, databases, applications, and deployment environments according to your permissions and instructions.

Agent activity may create logs, transcripts, traces, tool results, commands, screenshots, generated files, code changes, and deployment records.

SPIRITT may process this data to provide the Service, preserve context, enable resumption, debug issues, improve reliability, support users, detect abuse, and improve SPIRITT’s products, services, AI systems, evaluations, workflows, and safety systems.

Schedule 7. Connected Service Permissions

Permissions requested by SPIRITT depend on the Connected Service and features you choose. Permissions may include read, write, send, delete, admin, analytics, repository, cloud, calendar, email, file, messaging, advertising, or payment related permissions.

You can control authorization through the provider’s authorization screen, SPIRITT settings where available, and the Connected Service’s settings.

Revoking access may limit functionality. Revocation may not delete data already processed, stored, logged, included in Artifacts, or retained for legal, security, operational, or backup purposes.

Schedule 8. Google API Limited Use Disclosure

SPIRITT’s use and transfer of information received from Google APIs will adhere to the Google API Services User Data Policy, including Limited Use requirements.

SPIRITT uses Google user data only for purposes that are appropriate to the user facing features of the Service, including authentication, requested actions, file or data access requested by users, workflow execution, security, support, and service improvement where permitted.

SPIRITT does not use Google user data for unrelated advertising, does not sell Google user data, does not transfer Google user data to data brokers, and does not use Google user data for credit eligibility.

SPIRITT limits human access to Google user data except where permitted by Google policy, including user consent, security, legal compliance, or aggregated internal operations.

Schedule 9. Meta Platform Disclosure

SPIRITT processes Meta Platform Data only for disclosed purposes and according to permissions granted by users.

SPIRITT may use Meta Platform Data for authentication, account connection, user requested actions, analytics retrieval, asset management, security, support, abuse prevention, and compliance.

SPIRITT does not sell Meta Platform Data or process Meta Platform Data for undisclosed purposes.

Users may request deletion of Meta related data by contacting info@spiritt.io.

Schedule 10. Retention Criteria

SPIRITT determines retention periods based on the nature of the data, sensitivity of the data, purposes of processing, user settings, contractual requirements, legal obligations, security needs, dispute risk, backup cycles, operational requirements, and whether data is needed to provide the Service.

Account data may be retained while the account is active and for a reasonable period after closure. Billing records may be retained for tax and accounting purposes. Security logs may be retained to detect and investigate abuse. Backups may persist for a limited period according to backup cycles.

Aggregated, anonymized, or de identified data may be retained longer where permitted by law.

Schedule 11. Deletion Limitations

Deletion requests may be limited where data is needed for legal compliance, tax, accounting, security, fraud prevention, dispute resolution, contractual obligations, backups, audit logs, abuse prevention, or legitimate business purposes permitted by law.

Deletion of data from one system may not remove data from Connected Services, third party platforms, End User systems, public deployments, repositories, backups, logs, local exports, or Artifacts controlled by you.

If you are an End User of a SPIRITT customer, SPIRITT may need to refer your request to that customer.

Schedule 12. Security Measures

SPIRITT uses administrative, technical, and organizational measures designed to protect data. These may include access controls, credential management, authentication controls, encryption in transit where appropriate, monitoring, logging, vulnerability management, personnel controls, vendor review, and incident response processes.

Security measures vary by data type, product, customer configuration, provider, and risk. No method of transmission or storage is completely secure.

Users are responsible for account security, credential management, permission configuration, endpoint security, End User access, and backup practices.

Schedule 13. International Data Transfers

SPIRITT, its affiliates, and service providers may process data in the United States, Israel, the European Economic Area, the United Kingdom, and other locations where they operate.

Where required, SPIRITT relies on lawful transfer mechanisms, including adequacy decisions, standard contractual clauses, data processing agreements, contractual safeguards, or other mechanisms permitted by law.

Schedule 14. Controller and Processor Roles

SPIRITT may act as controller for account data, billing data, website data, support data, security data, service generated data, analytics data, and business operations data.

SPIRITT may act as processor or service provider when processing customer controlled personal data, including End User data, workspace content, files, application data, or Connected Service data on behalf of a business customer.

The role may vary depending on product, feature, customer agreement, data category, and processing purpose.

Schedule 15. Customer Responsibilities

Customers are responsible for providing privacy notices, obtaining consents, responding to End User rights requests, configuring permissions, limiting data collection, maintaining lawful bases, managing retention, and ensuring that their use of SPIRITT complies with applicable laws.

Customers are responsible for their Artifacts, End User relationships, Connected Services, and data submitted to the Service.

Schedule 16. US State Privacy Rights

Residents of certain US states may have rights to know, access, correct, delete, port, opt out of certain processing, restrict certain uses of sensitive data, or appeal denied requests.

SPIRITT will respond to applicable requests as required by law. SPIRITT may verify your identity and may deny requests where exceptions apply.

If SPIRITT processes data on behalf of a customer, SPIRITT may refer the request to the customer.

Schedule 17. California Notice

For California residents, SPIRITT may collect categories of personal information described in this Privacy Policy, including identifiers, commercial information, internet or network activity, approximate geolocation, professional information, inferences, sensitive information you choose to provide, and other information you provide or authorize.

SPIRITT uses and discloses these categories for the business and commercial purposes described in this Privacy Policy.

SPIRITT does not sell your User Content. If SPIRITT engages in activity considered a sale or sharing under California law, SPIRITT will provide required notices and choices.

California residents may contact info@spiritt.io to exercise applicable privacy rights.

Schedule 18. European Region and UK Notice

Where GDPR, UK GDPR, or similar laws apply, individuals may have rights to access, rectify, erase, restrict, object, port data, and withdraw consent.

SPIRITT may process data based on contract, legitimate interests, consent, legal obligations, vital interests, or legal claims.

Individuals may have the right to lodge a complaint with a supervisory authority.

SPIRITT may transfer data internationally using lawful transfer mechanisms.

Schedule 19. Israel Notice

Where Israeli privacy law applies, SPIRITT provides notice of the controller's identity and contact details, processing purposes, applicable rights, and consequences of refusing to provide data where required.

Some information is necessary to provide the Service. If you refuse to provide required information, SPIRITT may be unable to provide some or all of the Service.

Privacy questions may be sent to info@spiritt.io.

Schedule 20. Business Transfers

If SPIRITT is involved in a merger, acquisition, financing, reorganization, bankruptcy, receivership, sale of assets, corporate transaction, or transition of service to another provider, data may be disclosed, transferred, or processed as part of that transaction.

The acquiring or successor entity may continue to process data according to this Privacy Policy or a successor policy.

Schedule 21. Legal Requests

SPIRITT may disclose data in response to subpoenas, warrants, court orders, regulatory requests, law enforcement requests, legal process, or other legal obligations.

SPIRITT may also disclose data where it believes disclosure is reasonably necessary to protect rights, safety, property, security, users, End Users, third parties, or the public.

Schedule 22. Changes and Prior Versions

SPIRITT may update this Privacy Policy to reflect changes in the Service, law, data practices, providers, features, or business operations.

Material changes will be communicated where required. The effective date identifies the current version.

Continued use of the Service after an update means the updated policy applies to future use.

Schedule 23. Data Controls, Opt-Outs, and Temporary Modes

SPIRITT may provide data controls, opt-out settings, retention settings, temporary modes, workspace controls, enterprise controls, or privacy settings that affect how certain data is used or retained.

Available controls may vary by plan, workspace, feature, geography, provider, integration, and account type.

If a control is enabled, it may apply only to future data and may not affect data already processed, reviewed, aggregated, de identified, included in backups, retained in logs, used for security, or required for legal purposes.

Even if you opt out of certain improvement uses, SPIRITT may continue to process data to provide the Service, maintain safety and security, prevent abuse, comply with law, enforce terms, debug issues, provide support, and protect users, End Users, SPIRITT, or the public.

Schedule 24. Free, Trial, Paid, Business, and Enterprise Data Handling

Data handling may vary by plan or feature. Free, trial, beta, preview, evaluation, prototype, or unpaid features may involve broader logging, review, testing, analytics, safety analysis, and service improvement use than paid enterprise offerings.

Paid, business, enterprise, partner, or custom customers may receive additional data use restrictions, retention commitments, service levels, data processing terms, or security commitments under separate written agreements.

Unless a separate written agreement states otherwise, SPIRITT may use data as described in this Privacy Policy, including to improve SPIRITT's products, services, AI systems, evaluations, workflows, and safety systems.

Schedule 25. Connected App Summaries, Excerpts, and Inferences

When you connect third party apps or services, SPIRITT may process data from those services to respond to your requests, operate agents, personalize results, and perform actions.

SPIRITT may generate summaries, excerpts, embeddings, metadata, classifications, inferences, tool results, intermediate reasoning artifacts, logs, and derived data from Connected Service Data. These may be used to provide the Service, maintain context, improve quality, debug issues, protect against abuse, and improve SPIRITT's products, services, AI systems, evaluations, workflows, and safety systems where permitted.

Disconnecting a Connected Service may stop future access but may not delete summaries, excerpts, logs, inferences, Artifacts, or derived data already created or retained for permitted purposes.

Schedule 26. Human Review and Review Retention

SPIRITT may use trained personnel, contractors, reviewers, or service providers to review selected data for support, debugging, quality evaluation, policy enforcement, safety, abuse prevention, security, service improvement, or legal compliance.

Reviewed data may be retained for longer periods where necessary for quality, safety, security, compliance, dispute resolution, legal obligations, or service improvement.

SPIRITT may take steps to reduce personal information before review where appropriate and feasible, except where review is needed to address abuse, harm, security, support, legal compliance, or user request.

Schedule 27. Organization and Administrator Privacy

If your Account is part of an organization, team, company, domain, or enterprise workspace, administrators may access, control, export, delete, monitor, restrict, or manage data associated with the workspace.

Administrators may access User Content, Outputs, logs, usage information, Artifacts, Connected Services, settings, billing data, support data, security records, and user activity depending on the plan and configuration.

Your organization is responsible for providing required notices and obtaining required consents from users whose data may be accessed or controlled by administrators.

Schedule 28. Public Sharing and Published Content

If you share, publish, deploy, list, submit, or make content public through the Service, that content may be visible to others and may be indexed, copied, stored, downloaded, or redistributed by third parties.

SPIRITT may process public content to provide the Service, display the content, maintain public features, enforce policies, detect abuse, and improve the Service.

SPIRITT will not intentionally make private User Content public without your action, instruction, permission, or a legal or safety basis.

Schedule 29. Messaging and Communication Integrations

If you connect email, SMS, chat, social messaging, browser, calendar, voice, or other communication services, SPIRITT may process messages, metadata, attachments, recipients, sender information, timestamps, drafts, threads, and related context according to your permissions and instructions.

Some integrations may be limited to specific chats, threads, channels, accounts, labels, or sessions where technically feasible. Other integrations may require broader permissions based on provider design.

Third party communication platforms may process your data under their own terms and may restrict, suspend, or flag accounts based on automated activity or platform rules.

Schedule 30. Safety, Abuse Detection, and Policy Enforcement Data

SPIRITT may process Inputs, Outputs, logs, files, metadata, account data, usage patterns, device data, Connected Service Data, and Artifacts to detect, prevent, investigate, and respond to abuse, fraud, illegal activity, security threats, policy violations, harmful content, and attempts to bypass safeguards.

SPIRITT may use automated systems, human review, classifiers, reputation systems, rate limits, anomaly detection, and other controls for these purposes.

SPIRITT may preserve or disclose data where necessary to protect users, End Users, third parties, SPIRITT, or the public.

Schedule 31. Memories, Personalization, and Persistent Context

SPIRITT may provide memory, personalization, workspace history, retrieval, embeddings, preferences, summaries, project context, or similar features.

These features may store information about you, your workspace, your projects, your preferences, your prior instructions, or your interactions so the Service can provide more relevant responses and workflows.

You may have controls to manage or delete some memories or personalization data. Deleting a memory may not delete related logs, backups, Artifacts, support records, security records, or data already aggregated or de identified.

Schedule 32. Model Training, Evaluation, and AI Improvement

SPIRITT may use data described in this Privacy Policy to improve SPIRITT’s products, services, AI systems, evaluations, workflows, and safety systems unless restricted by a separate written agreement, supported settings, applicable law, or provider specific policy.

This may include model evaluation, prompt evaluation, workflow evaluation, agent behavior improvement, quality scoring, safety classification, synthetic data generation, red teaming, benchmarking, fine tuning where permitted, retrieval quality improvement, and development of new features.

SPIRITT may use aggregated, anonymized, de identified, or transformed data to reduce privacy risk where appropriate.

Schedule 33. Feedback, Reports, and Abuse Records

If you submit feedback, ratings, bug reports, corrections, abuse reports, support requests, or safety reports, SPIRITT may process the related content, conversation, logs, files, screenshots, tool results, and metadata to investigate the report, improve the Service, enforce policies, and develop safety systems.

Feedback and report data may be retained longer than ordinary content where needed for quality, safety, security, compliance, or dispute resolution.

SPIRITT may retain records of abusive, fraudulent, unsafe, or illegal activity as necessary to prevent repeat abuse, enforce policies, protect systems, respond to legal process, or protect third parties.

Schedule 34. Identity, Age, and Abuse Verification

SPIRITT may request or process identity, age, business, payment, domain, ownership, or authorization information where necessary to provide the Service, prevent abuse, comply with law, verify eligibility, support enterprise administration, or investigate suspicious activity.

Verification data may be processed by service providers and retained as necessary for legal, security, compliance, or fraud prevention purposes.

Schedule 35. Business Customer Processing Details

For business customers, the nature and purpose of processing is to provide, secure, support, maintain, and improve the Service, including AI workspaces, agents, automations, Artifacts, integrations, and related functionality.

The duration of processing is the term of the customer relationship and the period necessary afterward for deletion, backups, legal compliance, security, dispute resolution, and legitimate business purposes.

Categories of data subjects may include customer personnel, contractors, End Users, leads, customers, suppliers, applicants, partners, and other individuals whose data is submitted or connected by the customer.

Categories of personal data may include identifiers, contact information, account data, communications, files, code, business records, usage data, support data, and any other data submitted by the customer.

Sensitive data is not intended to be submitted unless the customer’s agreement permits it and required safeguards are in place.

Schedule 36. Subprocessors and Provider Changes

SPIRITT may use subprocessors and service providers to provide, secure, support, analyze, and improve the Service.

SPIRITT may update providers over time. SPIRITT will use reasonable measures designed to ensure providers process data according to appropriate confidentiality, security, and data protection obligations.

Where a customer has a separate DPA or enterprise agreement, subprocessor notice and objection rights, if any, will be governed by that agreement.

Schedule 37. Appeals, Complaints, and Rights Requests

You may contact SPIRITT at info@spiritt.io if you believe a privacy request was handled incorrectly, an account restriction was imposed in error, or content was removed in error.

SPIRITT may provide an appeal or review process where required by law or where appropriate. SPIRITT may decline review where doing so would create risk, reveal security methods, compromise an investigation, violate law, or affect third party rights.

Schedule 38. Automated Decision-Making

SPIRITT may use automated systems to operate the Service, detect abuse, prioritize support, classify content, recommend actions, route requests, generate Outputs, and secure the Service.

SPIRITT does not intend the Service to be used as the sole basis for decisions that produce legal or similarly significant effects without appropriate human review and legal compliance.

Customers using SPIRITT for such decisions are responsible for notices, consents, impact assessments, human review, appeal rights, and legal compliance.

Schedule 39. Data Minimization and User Responsibilities

You should submit only data necessary for your intended use. You are responsible for limiting sensitive, confidential, regulated, or unnecessary personal data in prompts, files, integrations, and Artifacts.

You are responsible for configuring agents, integrations, and workflows to access only data necessary for the task.

You are responsible for deleting or disconnecting data and integrations you no longer need, subject to retention limits described in this Privacy Policy.

Schedule 40. Contact Method and No Public Physical Address

SPIRITT provides privacy contact through info@spiritt.io.

SPIRITT may provide additional mailing addresses, registered agent details, regulatory contact details, or jurisdiction specific contacts where required by law, vendor requirements, regulator requests, or separate agreements.

Unless required by applicable law, SPIRITT may use electronic contact methods for privacy requests and notices.