SENEKA PRIVACY POLICY

SECTION 1 — INTRODUCTION / OVERVIEW

Privacy Policy

Last Updated: May 25, 2026

Welcome to Seneka.

This Privacy Policy explains how Seneka (“Seneka,” “we,” “our,” or “us”), operated by LUKAS INNOVATION GROUP LLC, a Wyoming limited liability company, collects, uses, stores, shares, and protects personal information when you access or use our websites, applications, products, tools, and related services.

This Privacy Policy applies to all Seneka services, including but not limited to:

- Seneka Labs;
- Seneka Workspace and SaaS features;
- Seneka Marketplace;
- Seneka Resources and educational content;
- public sharing pages and brand-related reports;
- mobile applications;
- web applications;
- APIs and integrations;
- all websites and domains operated by Seneka.

By accessing or using Seneka, you acknowledge that you have read and understood this Privacy Policy.

If you do not agree with this Privacy Policy, you should not access or use the Services.

Scope of Services

Seneka is a technology platform that may provide:

- AI-assisted trademark and brand analysis tools;

- legal workflow and collaboration features;
- attorney and client marketplace functionality;
- educational resources;
- subscription-based services;
- document and workspace management tools;
- public and private sharing functionality;
- analytics and reporting tools.

Some Seneka services may involve automated processing, AI-generated outputs, and interactions with third-party providers.

Additional privacy notices or disclosures may apply to certain services, integrations, jurisdictions, or products.

Important Notice About Legal Services

Seneka is not a law firm and does not provide legal advice.

Unless explicitly stated otherwise in a separate written agreement, communications through the platform do not create an attorney-client relationship between Seneka and any user.

AI-generated analyses, recommendations, scores, reports, or suggestions provided through Seneka are for informational purposes only and should not be relied upon as legal advice or legal opinion.

Users are solely responsible for independently evaluating any information generated through the Services before making legal, business, trademark, or commercial decisions.

International Users

Seneka may operate globally, and by using the Services, you understand that your information may be transferred to and processed in countries outside your country of residence, including the United States and other jurisdictions where our service providers operate.

Changes and Updates

We may update this Privacy Policy from time to time to reflect changes in our Services, legal obligations, technologies, or business practices.

When required by applicable law, we will provide notice of material changes.

The “Last Updated” date at the top of this Privacy Policy indicates when the latest revision became effective.

SECTION 2 — DEFINITIONS

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

“Seneka”

“Seneka,” “we,” “our,” or “us” refers to Seneka and its affiliated websites, applications, products, tools, services, and related operations, which are operated by LUKAS INNOVATION GROUP LLC, a Wyoming limited liability company.

“Platform”

“Platform” refers collectively to all Seneka-operated websites, applications, APIs, systems, products, technologies, tools, and related services, including but not limited to:

- Seneka Labs;
- Seneka Workspace;
- Seneka Marketplace;
- Seneka Resources;
- mobile applications;
- web applications;
- public sharing pages;
- integrations and APIs.

“Services”

“Services” refers to any features, products, functionality, content, tools, software, subscriptions, AI-powered systems, reports, marketplaces, or other services made available through the Platform.

“User”

“User” means any individual or entity who accesses, browses, registers for, interacts with, or otherwise uses the Platform or Services.

“Attorney”

“Attorney” refers to a lawyer, law firm, legal professional, trademark professional, or legal service provider who creates an account on the Platform or offers services through the Marketplace or related features.

“Client”

“Client” refers to any User seeking legal-related services, trademark assistance, consultations, attorney connections, or other professional support through the Platform or Marketplace.

“Marketplace”

“Marketplace” refers to any portion of the Platform that enables Users, Attorneys, law firms, professionals, or third parties to connect, communicate, collaborate, exchange information, offer services, or engage in transactions.

“Workspace”

“Workspace” refers to any private or shared digital environment, dashboard, account area, collaboration system, case management area, project space, or document environment made available through the Platform.

“AI Services”

“AI Services” refers to any artificial intelligence, machine learning, automated analysis, recommendation systems, scoring systems, generated reports, conversational interfaces, predictive tools, or automated processing features provided through the Platform.

AI Services may include AI-generated outputs, recommendations, classifications, summaries, scores, trademark analysis, risk indicators, or other automated content.

“Personal Data”

“Personal Data” means information that identifies, relates to, describes, could reasonably be associated with, or could reasonably be linked, directly or indirectly, to an identified or identifiable individual, household, or device, as defined under applicable privacy laws.

Personal Data may include, without limitation:

- name;
- email address;
- phone number;
- IP address;
- account information;
- billing information;
- device identifiers;
- uploaded content;
- communications;
- usage activity;
- business-related information;
- marketplace interactions.

“Content”

“Content” refers to any information, materials, text, trademarks, business names, files, documents, messages, uploads, prompts, reports, images, comments, communications, or other materials submitted to, generated through, or displayed on the Platform.

“Third-Party Services”

“Third-Party Services” refers to external products, providers, integrations, platforms, APIs, payment processors, analytics providers, hosting providers, AI providers, or other services that may interact with the Platform.

“Applicable Law”

“Applicable Law” means any law, regulation, rule, directive, ordinance, or legal requirement applicable to the processing of Personal Data or operation of the Services, including but not limited to privacy, consumer protection, and data protection laws.

SECTION 3 — INFORMATION WE COLLECT

Seneka may collect information directly from Users, automatically through the Platform, and from third-party sources in connection with providing and improving the Services.

The categories of information we collect depend on how you interact with the Platform, the Services you use, your account settings, and applicable legal requirements.

3.1 Information You Provide

We may collect information that you voluntarily provide when you create an account, use the Services, interact with the Platform, communicate with us, submit content, or engage with other Users.

Account Data

We may collect account-related information, including:

- full name;
- username;
- email address;
- phone number;
- password and authentication credentials;
- profile information;
- company or organization name;
- billing address;
- account preferences;
- subscription status;
- account verification information;
- profile photos or avatars;
- communication preferences.

We may also collect information related to authentication, security verification, fraud prevention, and account recovery.

Business Information

When using Seneka Labs, Workspace features, Marketplace functionality, or related Services, Users may provide business-related information, including:

- trademarks;
- proposed brand names;
- logos;
- slogans;
- business descriptions;
- industry classifications;
- trademark filing classes;
- filing strategies;
- search queries;
- business-related documents;
- brand evaluation materials;
- legal workflow information;
- intellectual property-related information;
- reports, notes, and research materials.

Certain Services may allow Users to generate, upload, analyze, store, or share trademark-related or business-related information using AI Services or collaborative tools.

Workspace Data

Users may upload, create, store, or share information within Workspaces or collaboration environments, including:

- documents;
- files;
- comments;
- case-related materials;
- notes;
- communications;
- uploads;
- internal workflow data;
- shared project information;
- task management information;
- messages and collaboration content;
- AI-generated reports or summaries.

Workspace data may include confidential, business-sensitive, or legal-related materials submitted by Users.

Marketplace Data

When Users interact through the Marketplace or attorney-related features, we may collect:

- attorney profiles;
- law firm information;
- client profiles;
- professional credentials;
- service listings;
- communications between Users;
- consultation requests;
- reviews and ratings;
- invoices;
- billing-related records;
- transaction-related information;
- scheduling information;
- dispute-related communications.

Users are solely responsible for the information they choose to share with Attorneys, Clients, or other Marketplace participants.

Communications and Support Requests

We may collect information when Users contact us or communicate through the Platform, including:

- customer support requests;
- feedback;
- survey responses;
- emails;
- chat communications;
- support tickets;
- dispute communications;
- communications with attorneys or marketplace participants.

AI Inputs and Generated Outputs

When Users interact with AI Services, we may collect:

- prompts;
- search requests;
- uploaded materials;
- generated reports;

- AI-generated responses;
- recommendations;
- automated analyses;
- risk assessments;
- classifications;
- summaries;
- feedback regarding AI outputs.

AI-generated outputs may be stored for service improvement, security, debugging, fraud prevention, analytics, and operational purposes, subject to applicable law and our agreements with third-party providers.

Public Sharing Content

If Users choose to use public sharing functionality, Seneka may collect and process information associated with publicly accessible pages, including:

- shared reports;
- brand names;
- public scorecards;
- shared summaries;
- public profile information;
- publicly generated URLs;
- engagement metrics.

Users are responsible for deciding what information they choose to make publicly accessible.

Payment Data

If you purchase subscriptions, paid reports, marketplace services, or other paid offerings, payment-related information may be processed by third-party payment processors.

Seneka does not store full payment card numbers, full banking credentials, or complete payment authentication data on its own servers.

Depending on the payment method and provider, we may receive limited payment-related information, such as:

- payment status;
- subscription status;
- billing identifiers;
- transaction confirmations;
- partial payment details;

- payment timestamps;
- invoice information.

Payments may be processed by third-party providers such as:

- Stripe;
- Paddle;
- RevenueCat;
- Apple App Store;
- Google Play;
- other authorized payment processors.

The collection and processing of payment information by third-party payment providers is governed by their respective privacy policies and terms.

3.2 Automatically Collected Information

When Users access or interact with the Platform, Seneka may automatically collect certain technical, device, usage, operational, and analytics-related information.

This information helps us operate, secure, maintain, analyze, improve, and personalize the Services.

Device & Technical Data

We may automatically collect technical and device-related information, including:

- IP address;
- approximate geographic location derived from IP address;
- browser type and version;
- device identifiers;
- device type;
- operating system and version;
- language preferences;
- time zone settings;
- internet service provider;
- mobile carrier information;
- hardware model;
- application version;
- referral URLs;
- access timestamps;
- session identifiers;
- authentication events;
- API request metadata;

- network and connection information;
- crash reports;
- error logs;
- performance diagnostics;
- debugging information;
- security and fraud-prevention signals.

For mobile applications, we may also collect limited mobile-device related information, such as:

- mobile operating system;
- application build/version;
- push notification token status;
- device configuration data;
- app interaction events;
- mobile diagnostics and stability information.

Usage Data

We may automatically collect information regarding how Users interact with the Platform and Services, including:

- pages visited;
- features accessed;
- tools used;
- workflows initiated;
- searches performed;
- reports generated;
- content viewed;
- interactions with AI Services;
- interactions with Marketplace features;
- workspace activity;
- navigation patterns;
- clicks, scrolls, and interactions;
- session duration;
- referring and exit pages;
- account activity;
- subscription interactions;
- engagement with emails or notifications;
- usage frequency and activity metrics.

We may also collect operational telemetry related to:

- AI-generated analysis requests;
- report generation events;
- workflow completion metrics;

- system performance;
- latency measurements;
- API activity;
- service reliability monitoring.

Cookies, Local Storage, and Similar Technologies

Seneka may use cookies, local storage objects, SDKs, pixels, tags, session technologies, and similar tracking technologies to:

- maintain sessions;
- remember user preferences;
- improve platform functionality;
- authenticate Users;
- prevent fraud and abuse;
- measure performance;
- analyze usage trends;
- personalize content and user experience;
- support analytics and operational monitoring.

Certain features of the Platform may not function properly if cookies or similar technologies are disabled.

Additional information regarding cookies and tracking technologies may be provided in a separate Cookie Policy or consent banner where required by applicable law.

Analytics and Monitoring Technologies

We may use internal analytics systems and third-party service providers to better understand how Users interact with the Platform and to improve the Services.

These technologies may collect information regarding:

- user engagement;
- feature usage;
- navigation behavior;
- conversion metrics;
- technical diagnostics;
- error tracking;
- crash analytics;
- service reliability;
- performance monitoring.

Third-party analytics or monitoring providers may include hosting, infrastructure, analytics, observability, communication, customer support, or AI-related providers.

Security and Fraud Prevention

We may automatically collect and analyze information for security, fraud prevention, abuse detection, platform integrity, and legal compliance purposes.

This may include:

- login attempts;
- authentication events;
- suspicious activity indicators;
- device consistency checks;
- rate-limiting data;
- automated abuse detection signals;
- network activity patterns;
- security event logs.

Seneka may use automated systems to detect unauthorized activity, spam, fraud, abuse, or violations of our Terms of Use.

AI Interaction Telemetry

When Users interact with AI Services, Seneka may automatically collect operational and diagnostic information related to AI usage, including:

- request timing;
- processing metadata;
- AI interaction events;
- model usage statistics;
- feedback signals;
- performance metrics;
- error diagnostics;
- output generation events;
- prompt interaction metadata.

Such information may be used to improve service reliability, optimize performance, maintain security, troubleshoot issues, and enhance AI-related functionality.

Aggregated and De-Identified Information

Seneka may generate aggregated, anonymized, or de-identified information that does not reasonably identify individual Users.

We may use such information for:

- analytics;
- research;
- product development;
- benchmarking;
- service improvement;
- operational reporting;
- security monitoring;
- business intelligence purposes.

SECTION 4 — HOW WE USE INFORMATION

Seneka may use Personal Data, technical information, usage information, Content, and other collected data for the purposes described in this Privacy Policy, as permitted by applicable law.

The specific ways in which we use information depend on the Services used, the nature of the interaction, legal obligations, operational requirements, and User settings.

Providing and Operating the Services

We use information to:

- provide access to the Platform and Services;
- create and manage User accounts;
- authenticate Users;
- maintain account functionality;
- operate Workspaces and collaboration environments;
- process transactions and subscriptions;
- deliver reports, analyses, and generated outputs;
- enable Marketplace functionality;
- facilitate attorney and client interactions;
- support integrations and APIs;
- provide mobile and web application functionality.

Authentication and Account Security

We use information for authentication, identity verification, account recovery, fraud prevention, abuse prevention, and platform security purposes.

This may include:

- verifying account ownership;
- monitoring login activity;
- detecting suspicious behavior;
- preventing unauthorized access;
- enforcing account protections;
- maintaining platform integrity;
- securing user sessions;
- protecting confidential information.

Fraud Prevention and Abuse Detection

Seneka may use automated and manual systems to detect, investigate, prevent, and respond to:

- fraud;
- spam;
- unauthorized activity;
- abuse of the Platform;
- intellectual property misuse;
- marketplace misconduct;
- payment-related abuse;
- suspicious transactions;
- violations of our Terms of Use;
- security threats and malicious activity.

AI Analysis and Automated Processing

Seneka may use Personal Data, User Content, prompts, uploaded materials, and interaction data to provide AI-powered functionality and automated processing features.

This may include:

- trademark risk analysis;
- brand analysis;
- classification systems;
- recommendation systems;

- report generation;
- AI-generated summaries;
- search assistance;
- scoring systems;
- predictive analysis;
- workflow automation;
- content organization;
- intelligent suggestions;
- AI-assisted legal workflow tools.

Certain AI Services may involve automated processing and machine-learning systems operated by Seneka or third-party AI providers.

Trademark Risk Analysis and Brand Evaluation

We may use information submitted through the Platform to:

- analyze trademark conflicts;
- evaluate brand distinctiveness;
- generate trademark-related reports;
- identify potential risks;
- assess classification relevance;
- generate business or legal-related insights;
- compare brand-related data;
- provide AI-assisted recommendations and evaluations.

Such analyses are informational in nature and are not legal advice.

Personalization and User Experience

We may use information to personalize and improve the User experience, including by:

- remembering preferences;
- customizing dashboards and Workspaces;
- improving recommendations;
- personalizing content;
- adapting interface behavior;
- optimizing workflows;
- suggesting relevant tools or features;
- improving Marketplace relevance;
- tailoring communications and notifications.

Subscription and Payment Management

We may use information to:

- manage subscriptions;
- process billing-related activity;
- verify payments;
- maintain transaction records;
- manage renewals and cancellations;
- detect payment fraud;
- provide invoices and receipts;
- administer premium Services.

Payment processing may be handled by authorized third-party payment providers.

Customer Support and Communications

We may use information to:

- respond to support requests;
- troubleshoot issues;
- provide technical assistance;
- communicate regarding accounts or Services;
- investigate disputes;
- respond to inquiries;
- send transactional notifications;
- provide operational or legal notices.

We may also send service-related communications necessary for operating the Platform.

Product Improvement and Research

We may use information to:

- improve existing Services;
- develop new features;
- improve system performance;
- optimize workflows;
- conduct testing and debugging;
- improve AI systems and platform functionality;
- analyze usage patterns;
- evaluate feature adoption;
- perform internal research and development;

- enhance reliability, scalability, and usability.

Where required by law, we will obtain appropriate consent before using Personal Data for certain purposes.

Analytics and Performance Monitoring

We may use information for analytics, operational intelligence, diagnostics, and monitoring purposes, including to:

- understand user behavior;
- measure engagement;
- evaluate performance metrics;
- monitor system reliability;
- detect technical issues;
- improve platform stability;
- optimize conversion and workflow efficiency;
- measure effectiveness of Services.

Legal Compliance and Protection of Rights

We may use information to:

- comply with legal obligations;
- enforce agreements and policies;
- respond to lawful requests;
- protect Users, Attorneys, Clients, and third parties;
- protect intellectual property rights;
- investigate legal claims;
- maintain regulatory compliance;
- prevent illegal activity;
- establish, exercise, or defend legal claims.

AI Services and Automated Decision-Making

Certain Services provided by Seneka involve artificial intelligence, machine learning systems, automated analysis, and algorithmic processing.

Users acknowledge and understand that:

- AI-generated outputs may contain inaccuracies, errors, omissions, outdated information, or incomplete analysis;
- AI-generated reports, scores, recommendations, classifications, or summaries may not reflect all legal, commercial, or factual considerations;
- automated systems may produce different results over time;
- AI outputs require independent human review and judgment;
- Users are solely responsible for evaluating and verifying AI-generated information before relying on it;
- AI-generated content should not be considered legal advice, legal opinion, trademark clearance, or professional legal representation.

Seneka is not a law firm and does not guarantee the accuracy, completeness, reliability, or legal sufficiency of AI-generated outputs.

Certain AI-related processing may involve third-party AI providers and automated systems operated on cloud infrastructure.

No Attorney-Client Relationship

Use of the Platform, including AI Services, Marketplace functionality, communications, generated reports, or attorney discovery tools, does not create an attorney-client relationship between Seneka and any User.

Any attorney-client relationship may exist solely between Users and independent Attorneys engaged outside or through the Marketplace under separate agreements.

Why This Processing Occurs

Seneka processes information for legitimate business, operational, legal, contractual, security, and service-related purposes, including maintaining a secure, reliable, scalable, and functional platform experience.

Depending on the jurisdiction and applicable law, processing may rely on one or more legal bases described in this Privacy Policy.

SECTION 5 — LEGAL BASES FOR PROCESSING (GDPR)

If you are located in the European Economic Area (“EEA”), United Kingdom, or another jurisdiction requiring a lawful basis for processing Personal Data, Seneka processes Personal Data only where a valid legal basis exists under applicable law.

Depending on the nature of the Services used and the context of the processing, Seneka may rely on one or more of the following legal bases.

Contractual Necessity

We may process Personal Data when necessary to:

- provide the Services requested by Users;
- create and maintain accounts;
- operate Workspaces and Marketplace functionality;
- provide AI-powered tools and reports;
- process transactions and subscriptions;
- authenticate Users;
- provide customer support;
- fulfill contractual obligations;
- enforce our Terms of Use and related agreements;
- administer billing and payments;
- maintain platform functionality.

Without certain Personal Data, some Services may not function properly or may be unavailable.

Legitimate Interests

We may process Personal Data where necessary for our legitimate business interests, provided such interests are not overridden by Users’ fundamental rights and freedoms.

Legitimate interests may include:

- operating and improving the Platform;
- platform administration;
- fraud prevention and abuse detection;
- cybersecurity and platform integrity;
- analytics and performance monitoring;
- AI system improvement and optimization;

- service reliability and troubleshooting;
- internal reporting and operational analytics;
- feature development;
- Marketplace safety and moderation;
- communication regarding Services;
- protecting legal rights and interests;
- preventing unauthorized activity;
- enforcing our agreements and policies.

When relying on legitimate interests, we consider the potential impact on Users and implement appropriate safeguards where required.

Consent

We may process Personal Data based on User consent where required by applicable law.

This may include consent relating to:

- certain cookies and tracking technologies;
- marketing communications;
- optional features;
- AI-related functionality where legally required;
- mobile permissions;
- location-based functionality;
- push notifications;
- participation in surveys or promotional activities.

Users may withdraw consent at any time where processing is based on consent.

Withdrawal of consent does not affect the lawfulness of processing conducted prior to withdrawal.

Legal Obligations

We may process Personal Data when necessary to comply with applicable legal obligations, including obligations related to:

- financial and tax reporting;
- fraud prevention;
- anti-money laundering requirements;
- consumer protection laws;
- court orders and legal requests;
- regulatory compliance;
- law enforcement requests;

- dispute resolution;
- legal claims and investigations;
- recordkeeping requirements;
- security obligations.

Protection of Rights and Security

We may process Personal Data where necessary to:

- protect the rights, safety, and security of Users, Attorneys, Clients, third parties, or the Platform;
- detect and prevent fraud or unauthorized activity;
- investigate abuse or policy violations;
- maintain platform integrity;
- protect intellectual property rights;
- respond to security incidents or threats.

Automated Processing and AI Systems

Certain Services involve automated processing and AI-assisted systems.

Where required by applicable law, Seneka will implement appropriate safeguards relating to automated processing and AI-related decision-support systems.

AI-generated outputs are intended to assist Users and should not be relied upon as a substitute for independent legal or professional judgment.

International Processing

Users understand that Personal Data may be processed and transferred internationally where necessary to operate the Services, provide infrastructure, support integrations, maintain security, and deliver AI-powered functionality.

Appropriate safeguards may be implemented where required under applicable data protection laws.

Data Minimization and Proportionality

Seneka seeks to limit the collection and processing of Personal Data to information reasonably necessary for the purposes described in this Privacy Policy.

We may also implement technical, administrative, and organizational safeguards designed to reduce unnecessary processing and protect User privacy.

Privacy Contact

Privacy and data protection requests may be submitted using the contact information provided in Section 19 of this Privacy Policy.

SECTION 6 — SHARING OF INFORMATION

Seneka may share Personal Data and other information in limited circumstances described in this Privacy Policy, where reasonably necessary to operate the Services, comply with legal obligations, protect rights and security, facilitate Marketplace functionality, or support business operations.

We do not sell Personal Data in exchange for monetary compensation.

6.1 Service Providers and Infrastructure Partners

Seneka may share information with trusted third-party vendors, contractors, service providers, and infrastructure partners that perform services on our behalf or support operation of the Platform.

These providers may assist with:

- cloud hosting and infrastructure;
- data storage;
- content delivery;
- analytics and monitoring;
- payment processing;
- subscription management;
- customer support;
- communication services;

- authentication and security;
- fraud prevention;
- AI and machine learning services;
- email delivery;
- push notifications;
- performance optimization;
- crash reporting;
- logging and diagnostics;
- legal compliance and auditing.

Examples of categories of providers may include:

- hosting and cloud infrastructure providers;
- analytics and observability providers;
- payment processors;
- mobile platform providers;
- AI service providers;
- customer support systems;
- communication and email delivery providers;
- security and anti-abuse providers.

These third parties may access Personal Data only as reasonably necessary to perform services on our behalf and subject to contractual, technical, or legal restrictions where applicable.

6.2 Marketplace, Attorneys, and User Interactions

Certain Services may allow Users, Attorneys, law firms, Clients, or other participants to communicate, collaborate, exchange documents, or share information through the Platform or Marketplace functionality.

Information shared through such interactions may include:

- profile information;
- communications;
- uploaded documents;
- consultation details;
- invoices;
- legal-related materials;
- business information;
- marketplace activity.

Users are solely responsible for the information they choose to share with Attorneys, Clients, law firms, or other Users.

Seneka does not control, monitor, verify, endorse, supervise, or guarantee the conduct, qualifications, licensing, advice, communications, or actions of Attorneys, Clients, or Marketplace participants.

Seneka is not responsible for:

- legal advice provided by third parties;
- attorney conduct;
- professional services;
- client interactions;
- disputes between Users;
- marketplace communications;
- external agreements between Users and Attorneys.

Any attorney-client relationship exists solely between Users and independent Attorneys under separate agreements.

6.3 Legal Compliance and Protection of Rights

Seneka may disclose information where we reasonably believe disclosure is necessary to:

- comply with applicable law;
- respond to lawful requests;
- comply with subpoenas, court orders, or legal process;
- respond to law enforcement or regulatory requests;
- investigate fraud, abuse, security incidents, or illegal activity;
- enforce our agreements, Terms of Use, or policies;
- protect the rights, safety, property, or security of Users, Attorneys, Clients, third parties, or the Platform;
- establish, exercise, or defend legal claims;
- prevent harm or unauthorized activity.

Where permitted by applicable law, we may attempt to notify affected Users regarding legal requests involving their information.

6.4 Business Transfers and Corporate Transactions

Seneka may disclose, transfer, or share information in connection with an actual or proposed:

- merger;
- acquisition;
- financing transaction;
- investment transaction;
- asset sale;
- reorganization;
- restructuring;
- bankruptcy;
- dissolution;
- corporate transaction;
- due diligence process.

In such circumstances, Personal Data and other information may be transferred as part of the transaction, subject to applicable confidentiality obligations and legal requirements.

6.5 Third-Party Integrations and External Services

Certain features of the Platform may integrate with or rely upon third-party services, platforms, APIs, or external providers.

If Users choose to connect or interact with third-party integrations, certain information may be shared as necessary to provide the requested functionality.

Use of third-party services is subject to the privacy policies and terms of those third parties.

Seneka is not responsible for the privacy, security, or data practices of third-party services that are not owned or controlled by Seneka.

6.6 Publicly Shared Content

Information intentionally made public by Users through public sharing functionality may become accessible to other Users, third parties, search engines, or the general public.

This may include:

- public share pages;
- shared reports;
- public scorecards;
- profile information;
- shared summaries;
- public links.

Users are responsible for determining what information they choose to make publicly available through the Platform.

6.7 Aggregated and De-Identified Information

Seneka may share aggregated, anonymized, statistical, or de-identified information that does not reasonably identify individual Users.

Such information may be used for:

- analytics;
- benchmarking;
- operational reporting;
- research;
- product improvement;
- business intelligence;
- security monitoring;
- industry analysis.

Why We Share Information

We share information only where reasonably necessary to:

- operate the Platform;
- provide Services;
- support Marketplace functionality;
- maintain security;
- comply with legal obligations;
- improve products and infrastructure;
- support transactions and subscriptions;
- protect Users and the Platform.

SECTION 7 — INTERNATIONAL DATA TRANSFERS

Seneka may operate globally, and the Services may be accessed by Users from different countries and jurisdictions.

As a result, Personal Data and other information may be transferred to, stored in, accessed from, or processed in countries outside the User's country of residence, including countries that may have different data protection laws than those in the User's jurisdiction.

This includes transfers to and processing within:

- the United States;
- countries within the European Economic Area ("EEA");
- the United Kingdom;
- cloud infrastructure regions;
- jurisdictions where our service providers, infrastructure providers, payment providers, analytics providers, AI providers, or affiliates operate.

Cross-Border Transfers

By using the Platform or Services, Users understand and acknowledge that information may be transferred internationally as necessary to:

- operate the Platform;
- provide Services;
- process transactions;
- support AI functionality;
- maintain infrastructure;
- store data;
- provide analytics and monitoring;
- support Marketplace functionality;
- facilitate customer support;
- maintain security and fraud prevention systems;
- support integrations and third-party providers.

Certain providers used by Seneka may process information across multiple jurisdictions.

Service Providers and Global Infrastructure

Seneka may use third-party providers and infrastructure partners located in different countries, including providers relating to:

- cloud hosting;
- content delivery;
- analytics;
- monitoring;
- payment processing;
- communications;
- customer support;
- AI and machine learning systems;
- security and anti-fraud systems;
- mobile platform infrastructure;
- operational tooling.

These providers may process Personal Data on servers located outside a User's jurisdiction.

Standard Contractual Clauses and Safeguards

Where required under applicable law, Seneka may rely on legally recognized transfer mechanisms and safeguards for international data transfers, including:

- Standard Contractual Clauses ("SCCs");
- contractual protections;
- data processing agreements;
- organizational safeguards;
- technical safeguards;
- access controls;
- security measures;
- other lawful transfer mechanisms recognized under applicable law.

Seneka may also take reasonable steps to assess whether recipients of transferred data provide an adequate level of data protection consistent with applicable legal requirements.

Reasonable Safeguards

Seneka seeks to implement reasonable administrative, technical, contractual, and organizational safeguards designed to protect Personal Data during international transfer, storage, and processing activities.

Such safeguards may include:

- encryption measures;
- restricted access controls;
- authentication protections;
- security monitoring;
- contractual confidentiality obligations;
- vendor assessments;
- logging and incident monitoring;
- data minimization practices;
- infrastructure security controls.

No method of transmission, storage, or processing is completely secure, and Seneka cannot guarantee absolute security.

International AI Processing

Certain AI Services and automated processing features may involve international processing by AI providers, cloud infrastructure providers, or machine learning systems operating across multiple jurisdictions.

AI-related processing may include temporary storage, processing, transmission, or analysis of prompts, uploaded content, generated outputs, and interaction metadata where necessary to provide AI-powered functionality.

Users should avoid submitting information they do not wish to be processed through AI-enabled systems.

EEA, UK, and Similar Jurisdictions

If you are located in the EEA, United Kingdom, or another jurisdiction with international transfer restrictions, you understand that your information may be transferred outside your jurisdiction where necessary to operate the Services.

Where required by law, Seneka will implement appropriate safeguards intended to provide an adequate level of protection for transferred Personal Data.

User Acknowledgment

By accessing or using the Services, Users acknowledge and understand that international transfers of information may occur as described in this Privacy Policy.

SECTION 8 — DATA RETENTION

Seneka retains Personal Data and other information only for as long as reasonably necessary to fulfill the purposes described in this Privacy Policy, provide the Services, comply with legal obligations, resolve disputes, enforce agreements, maintain security, and support legitimate business operations.

Retention periods may vary depending on the nature of the information, the Services used, legal requirements, operational needs, and applicable contractual obligations.

General Retention Principles

Seneka may retain information for purposes including:

- maintaining User accounts;
- operating the Platform and Services;
- supporting Workspaces and Marketplace functionality;
- processing subscriptions and transactions;
- maintaining security and fraud prevention systems;
- preserving business and operational records;
- troubleshooting and debugging;
- enforcing agreements and policies;
- complying with legal and regulatory obligations;
- resolving disputes;
- protecting legal rights and interests.

When information is no longer reasonably necessary, Seneka may delete, anonymize, aggregate, de-identify, or securely dispose of such information in accordance with applicable law and operational requirements.

Account Information

Account-related information may be retained while a User account remains active.

Following account closure or deletion requests, Seneka may retain limited information for purposes including:

- fraud prevention;
- security monitoring;
- dispute resolution;

- legal compliance;
- tax and accounting obligations;
- enforcing agreements;
- preventing abuse or unauthorized re-registration;
- maintaining operational integrity.

Workspace and Marketplace Data

Workspace materials, communications, uploaded content, Marketplace records, invoices, transaction-related information, and collaboration data may be retained for reasonable operational, legal, security, compliance, and contractual purposes.

Retention periods may vary depending on:

- the type of Service used;
- legal obligations;
- dispute-related requirements;
- contractual commitments;
- security considerations;
- regulatory obligations;
- business continuity requirements.

AI Interaction Data and Generated Outputs

AI-related interaction data, prompts, generated outputs, reports, and operational metadata may be retained for limited periods for purposes including:

- service functionality;
- security;
- fraud prevention;
- debugging;
- analytics;
- reliability monitoring;
- operational improvement;
- performance optimization;
- abuse detection;
- legal compliance.

Where possible and appropriate, Seneka may de-identify, aggregate, anonymize, or minimize AI-related operational data.

Analytics, Logs, and Security Records

Seneka may retain:

- technical logs;
- authentication records;
- analytics information;
- operational telemetry;
- crash reports;
- performance diagnostics;
- audit records;
- fraud-prevention signals;
- security event logs.

Retention periods for such information may vary depending on operational, legal, compliance, fraud prevention, and security requirements.

Payment and Transaction Records

Certain billing, subscription, invoice, and transaction-related information may be retained as necessary to:

- comply with tax laws;
- comply with accounting requirements;
- prevent fraud;
- resolve disputes;
- maintain financial records;
- comply with regulatory obligations.

Payment card information is generally processed by third-party payment processors and not stored directly by Seneka.

Backup and Disaster Recovery Systems

Seneka may maintain backup copies of information for disaster recovery, security, operational continuity, and infrastructure reliability purposes.

Backup systems may temporarily retain information after deletion requests or account closure until such backups are securely overwritten, deleted, rotated, or expire according to operational schedules.

Account Deletion and Deactivation

Users may request deletion of their accounts, subject to applicable law and operational limitations.

Upon account deletion or approved deletion request:

- access to the account may be disabled;
- certain information may be removed or anonymized;
- publicly visible information may be deleted or hidden where reasonably feasible;
- some information may remain retained for legal, security, fraud prevention, accounting, operational, contractual, or regulatory purposes.

Seneka may retain limited information after deletion requests where necessary to:

- comply with legal obligations;
- resolve disputes;
- enforce agreements;
- maintain security;
- prevent fraud or abuse;
- protect legal rights;
- comply with financial or tax obligations.

Deletion Timelines

Where reasonably practicable and subject to applicable legal obligations, Seneka aims to process account deletion requests within a commercially reasonable timeframe.

Certain data may persist temporarily in:

- backups;
- logs;
- disaster recovery systems;
- archived systems;
- operational records;
- legal compliance records.

Retention and deletion timelines may vary depending on technical, operational, contractual, legal, or regulatory requirements.

De-Identified and Aggregated Information

Seneka may retain anonymized, aggregated, statistical, or de-identified information that does not reasonably identify individual Users.

Such information may be retained for:

- analytics;
- benchmarking;
- operational reporting;
- AI system improvement;
- research;
- product development;
- business intelligence;
- security monitoring.

Legal Retention Requirements

In certain circumstances, Seneka may be required to retain information for longer periods to comply with:

- applicable law;
- legal process;
- regulatory obligations;
- court orders;
- tax requirements;
- accounting obligations;
- fraud prevention obligations;
- law enforcement requests;
- dispute resolution requirements.

SECTION 9 — DATA SECURITY

Seneka implements and maintains administrative, technical, organizational, and physical safeguards designed to help protect Personal Data and other information against unauthorized access, disclosure, alteration, misuse, loss, destruction, or other unauthorized processing.

Our security practices are designed to support the confidentiality, integrity, availability, and resilience of the Platform and Services.

Security Measures

Depending on the nature of the Services and processing activities, Seneka may implement security measures including:

- encryption technologies;
- secure communication protocols;
- access controls;
- authentication mechanisms;
- role-based access restrictions;
- account security protections;
- infrastructure monitoring;
- logging and auditing systems;
- security event monitoring;
- network protections;
- system hardening;
- backup and recovery procedures;
- operational safeguards;
- vulnerability management;
- incident detection mechanisms;
- fraud prevention systems;
- anti-abuse protections;
- data minimization practices;
- internal confidentiality controls.

Security measures may evolve over time as technologies, threats, legal requirements, and operational practices change.

Encryption and Secure Transmission

Seneka may use encryption and secure transmission technologies designed to protect information during transmission and storage where appropriate.

This may include:

- encrypted communications;
- HTTPS/TLS protections;
- encrypted storage systems;
- secure infrastructure environments;
- protected authentication workflows.

Certain third-party providers used by Seneka may also implement independent security measures and encryption technologies.

Access Controls

Access to Personal Data and sensitive systems is intended to be limited to authorized personnel, contractors, vendors, or service providers who reasonably require such access for legitimate operational purposes.

Seneka may implement:

- role-based permissions;
- authentication controls;
- access logging;
- administrative restrictions;
- internal authorization procedures;
- security reviews.

Unauthorized access or use of the Platform is prohibited.

Monitoring and Security Operations

Seneka may monitor systems, infrastructure, operational telemetry, authentication activity, API usage, Marketplace activity, and security events for purposes including:

- detecting suspicious activity;
- preventing fraud and abuse;
- maintaining platform integrity;
- identifying vulnerabilities;
- investigating security incidents;
- protecting Users and the Services;
- improving operational resilience.

Certain monitoring activities may involve automated detection systems and third-party infrastructure or security providers.

User Responsibilities

Users are responsible for helping maintain the security of their accounts and information.

Users should:

- maintain strong passwords;
- protect authentication credentials;
- avoid unauthorized sharing of account access;
- promptly report suspected unauthorized activity;
- use secure devices and networks where possible;

- exercise caution when sharing information through the Platform or Marketplace.

Seneka is not responsible for unauthorized access resulting from User failure to maintain appropriate account security practices.

Third-Party Services and Infrastructure

Certain Services may rely on third-party providers, including:

- cloud infrastructure providers;
- payment processors;
- AI providers;
- analytics providers;
- communication services;
- Marketplace integrations;
- customer support systems.

While Seneka seeks to work with reputable providers and implement reasonable safeguards, we do not control the independent security practices of third parties.

Users acknowledge that third-party services may involve separate security practices and risks.

Incident Response and Security Investigations

Seneka may investigate suspected security incidents, unauthorized activity, fraud, abuse, or violations of applicable agreements and policies.

Where required by applicable law, Seneka may provide notifications regarding certain security incidents or data breaches.

Notification timing and content may depend on:

- legal obligations;
- law enforcement considerations;
- operational requirements;
- technical circumstances;
- risk assessments.

No Absolute Security Guarantee

Although Seneka seeks to implement reasonable safeguards and security practices, no method of transmission, storage, processing, or electronic system can be guaranteed to be completely secure.

Accordingly:

- Seneka cannot guarantee absolute security;
- Users transmit information at their own risk;
- security measures may not prevent all unauthorized access, disclosure, misuse, or security incidents;
- internet-based services inherently involve certain security risks.

To the fullest extent permitted by applicable law, Seneka disclaims liability for unauthorized access, loss, disclosure, alteration, or destruction of information resulting from circumstances beyond our reasonable control.

Security Improvements and Evolving Practices

Seneka may update, modify, improve, or replace security practices, technologies, safeguards, and operational procedures over time in response to:

- evolving threats;
- technological developments;
- legal and regulatory requirements;
- operational needs;
- infrastructure changes;
- industry practices.

Security Reporting

If you believe you have identified a security vulnerability, unauthorized access issue, or security-related concern involving the Platform or Services, you may contact:

security@senekalegal.com

SECTION 10 — YOUR PRIVACY RIGHTS

Depending on your jurisdiction, applicable law, and the nature of your interaction with the Platform, you may have certain rights regarding your Personal Data.

Seneka is committed to respecting applicable privacy and data protection rights, including rights provided under the GDPR, UK GDPR, CCPA, CPRA, and similar privacy laws.

10.1 GDPR and Similar Privacy Rights

If you are located in the European Economic Area (“EEA”), United Kingdom, or another jurisdiction providing similar protections, you may have the following rights, subject to applicable legal limitations and exceptions.

Right to Access

You may request access to Personal Data that Seneka processes about you, including information regarding:

- categories of data collected;
- purposes of processing;
- categories of recipients;
- retention practices;
- sources of information;
- applicable safeguards for international transfers.

Right to Correction

You may request correction of inaccurate or incomplete Personal Data maintained by Seneka.

Users may also update certain account information directly through account settings or Workspace controls where available.

Right to Deletion

You may request deletion of Personal Data in certain circumstances, subject to legal, operational, contractual, fraud prevention, security, accounting, or regulatory retention requirements.

Deletion requests may not result in immediate removal from backups, logs, archived systems, or legal compliance records.

Right to Restrict Processing

You may request restriction of certain processing activities under circumstances permitted by applicable law.

Where processing is restricted, Seneka may continue storing certain information where legally permitted.

Right to Object

You may object to certain processing activities based on legitimate interests or direct marketing activities where applicable under law.

Seneka may continue certain processing where compelling legitimate grounds or legal obligations exist.

Right to Data Portability

Where legally applicable, you may request a copy of certain Personal Data in a structured, commonly used, and machine-readable format.

Portability rights apply only in limited circumstances under applicable law.

Right to Withdraw Consent

Where processing is based on consent, you may withdraw consent at any time.

Withdrawal of consent does not affect processing conducted before withdrawal.

Certain Services or features may become unavailable if consent is withdrawn.

Right to Lodge a Complaint

Users located in jurisdictions with applicable privacy rights may have the right to lodge complaints with relevant supervisory or regulatory authorities.

10.2 California Privacy Rights (CCPA / CPRA)

If you are a California resident, you may have certain rights under the California Consumer Privacy Act (“CCPA”) and California Privacy Rights Act (“CPRA”), subject to applicable limitations and exceptions.

Right to Know

You may request information regarding:

- categories of Personal Data collected;
- categories of sources;
- purposes for collection and use;
- categories of third parties with whom information is shared;
- categories of information disclosed;
- categories of information retained.

Right to Access

You may request access to specific pieces of Personal Data collected about you, subject to verification requirements and legal limitations.

Right to Correct

You may request correction of inaccurate Personal Data maintained by Seneka.

Right to Delete

You may request deletion of Personal Data collected from you, subject to applicable legal exceptions and operational requirements.

Right to Non-Discrimination

Seneka will not unlawfully discriminate against Users for exercising privacy rights provided under applicable law.

However, certain features or Services may require specific information to function properly.

Right to Limit Certain Uses of Sensitive Information

Where applicable under law, Users may have rights relating to certain categories of sensitive information.

Seneka does not use sensitive personal information for purposes requiring additional opt-out rights under CPRA beyond those reasonably necessary to provide the Services.

Right to Opt-Out of Certain Data Sharing

Where applicable, Users may have the right to opt out of certain forms of targeted advertising, profiling, or sharing activities as defined under applicable law.

Seneka currently does not sell Personal Data in exchange for monetary compensation.

No Sale of Personal Data

Seneka does not sell Personal Data to third parties for monetary compensation.

Seneka also does not knowingly engage in the sale of Personal Data of minors under applicable law.

Certain limited disclosures to service providers, analytics providers, infrastructure providers, or operational partners may constitute “sharing” under certain privacy laws, but such disclosures are made for operational, business, security, analytics, or service-related purposes.

10.3 Exercising Privacy Rights

Users may submit privacy-related requests using the contact information provided in Section 19 of this Privacy Policy.

To protect privacy and security, Seneka may:

- verify identity;
- request additional information;
- authenticate account ownership;
- decline requests where legally permitted;
- limit repetitive or abusive requests.

Authorized agents acting on behalf of Users may be required to provide proof of authorization where required by law.

10.4 Response Timing

Seneka will seek to respond to verified privacy requests within timeframes required by applicable law.

Response timing may vary depending on:

- the complexity of the request;
- legal obligations;
- technical limitations;
- operational requirements;
- identity verification procedures.

10.5 Limitations and Exceptions

Certain rights may be limited or unavailable where permitted under applicable law, including where processing is necessary for:

- legal compliance;
- fraud prevention;
- security;
- contractual obligations;
- protection of rights;
- dispute resolution;
- tax or accounting requirements;
- legal claims;
- operational continuity;
- public interest obligations.

10.6 Appeals and Additional Rights

Where required by applicable law, Users may have the right to appeal certain privacy-related decisions or request additional review of denied requests.

Information regarding appeals procedures may be provided where applicable.

SECTION 11 — CALIFORNIA PRIVACY NOTICE

This California Privacy Notice supplements the other sections of this Privacy Policy and applies solely to residents of California to the extent required under the California Consumer Privacy Act (“CCPA”), as amended by the California Privacy Rights Act (“CPRA”), and other applicable California privacy laws.

This section describes how Seneka collects, uses, retains, discloses, and processes Personal Data relating to California residents.

11.1 Categories of Personal Data Collected

During the preceding twelve (12) months, Seneka may have collected the following categories of Personal Data, depending on how Users interact with the Platform and Services:

Identifiers

Examples may include:

- name;
- email address;
- phone number;

- account identifiers;
- username;
- IP address;
- device identifiers;
- online identifiers.

Customer and Account Information

Examples may include:

- billing-related information;
- subscription information;
- account preferences;
- profile information;
- customer support interactions;
- transaction-related information.

Commercial Information

Examples may include:

- subscription activity;
- purchases;
- transaction history;
- invoices;
- Marketplace interactions;
- service usage history.

Internet and Electronic Activity Information

Examples may include:

- browsing activity;
- pages visited;
- interactions with the Platform;
- analytics information;
- searches;
- reports generated;
- usage metrics;
- interactions with AI Services;
- operational telemetry.

Geolocation Information

Examples may include:

- approximate location derived from IP address;
- device region information;
- general geographic indicators.

Seneka does not knowingly collect precise geolocation information unless specifically enabled through optional features or device permissions.

Professional or Employment-Related Information

Examples may include:

- attorney profiles;
- law firm information;
- professional credentials;
- Marketplace participation;
- business affiliations.

User Content and Uploaded Materials

Examples may include:

- trademarks;
- business names;
- uploaded documents;
- Workspace materials;
- communications;
- prompts submitted to AI Services;
- generated reports;
- collaboration data.

Inferences and Generated Insights

Examples may include:

- usage patterns;

- recommendations;
- AI-generated analyses;
- workflow insights;
- engagement metrics;
- system-generated classifications.

11.2 Business and Commercial Purposes

Seneka may collect, use, retain, disclose, or process Personal Data for business and commercial purposes including:

- providing and operating the Services;
- account management;
- authentication and security;
- fraud prevention;
- subscription management;
- Marketplace functionality;
- AI-powered analysis and reporting;
- trademark analysis;
- personalization;
- analytics and diagnostics;
- customer support;
- operational improvement;
- infrastructure maintenance;
- legal compliance;
- protection of rights and security;
- research and development;
- monitoring platform performance.

Additional details regarding processing purposes are described throughout this Privacy Policy.

11.3 Categories of Sources

Seneka may collect Personal Data from:

- Users directly;
- devices and browsers;
- Marketplace interactions;
- Workspace activity;
- AI Service interactions;

- payment and subscription providers;
- analytics providers;
- communication systems;
- integrations and APIs;
- third-party service providers;
- automated technologies.

11.4 Categories of Third Parties With Whom Information May Be Shared

Seneka may disclose Personal Data to categories of recipients including:

- service providers;
- cloud infrastructure providers;
- analytics providers;
- payment processors;
- AI providers;
- customer support providers;
- communication providers;
- security and fraud-prevention providers;
- Marketplace participants;
- legal or regulatory authorities where required;
- advisors, auditors, or professional service providers;
- parties involved in corporate transactions.

Additional details regarding disclosures are described elsewhere in this Privacy Policy.

11.5 Retention Practices

Seneka retains Personal Data only for as long as reasonably necessary for the purposes described in this Privacy Policy, including:

- operational purposes;
- legal compliance;
- fraud prevention;
- security;
- contractual obligations;
- dispute resolution;
- tax and accounting obligations;
- business continuity;

- enforcement of agreements.

Retention periods vary depending on the type of information, the Services used, and applicable legal requirements.

Additional details regarding retention are described in the Data Retention section of this Privacy Policy.

11.6 Sensitive Personal Information

Seneka may process limited categories of information that could be considered “sensitive personal information” under California law, depending on how Users interact with the Services.

Such information may include:

- account credentials;
- authentication-related information;
- certain communications;
- business-sensitive materials uploaded by Users.

Seneka does not use or disclose sensitive personal information for purposes that would require a separate “Limit the Use of My Sensitive Personal Information” right under CPRA beyond uses reasonably necessary to provide the Services, maintain security, comply with law, or operate the Platform.

11.7 No Sale of Personal Data

Seneka does not sell Personal Data in exchange for monetary compensation.

Seneka also does not knowingly sell or share the Personal Data of individuals under sixteen (16) years of age.

Certain limited disclosures to analytics providers, infrastructure providers, operational service providers, or advertising-related technologies may be considered “sharing” under California law depending on regulatory interpretation.

11.8 California Privacy Rights

California residents may have rights under applicable law, including rights to:

- know;
- access;
- correct;
- delete;
- limit certain uses of sensitive information;
- opt out of certain sharing activities;
- receive information regarding disclosures;
- non-discrimination for exercising privacy rights.

Additional information regarding these rights is described in the “Your Privacy Rights” section of this Privacy Policy.

11.9 Exercising California Privacy Rights

California residents may submit privacy-related requests through designated privacy contact methods described in this Privacy Policy.

Seneka may verify identity before processing requests and may deny requests where permitted by applicable law.

Authorized agents may be required to provide documentation demonstrating authority to act on behalf of a User.

11.10 California “Shine the Light” Disclosure

California residents may have rights under California Civil Code Section 1798.83 regarding certain disclosures of Personal Data to third parties for direct marketing purposes.

Seneka does not currently disclose Personal Data to third parties for their own direct marketing purposes in exchange for monetary compensation.

SECTION 12 — EU / UK PRIVACY RIGHTS

This section applies to Users located in the European Economic Area (“EEA”), United Kingdom (“UK”), Switzerland, and other jurisdictions that provide similar privacy and data protection rights under applicable law.

Seneka seeks to process Personal Data in accordance with applicable data protection laws, including the General Data Protection Regulation (“GDPR”), the UK GDPR, and related legal frameworks where applicable.

12.1 Data Protection Rights

Subject to applicable law and certain limitations, Users located in the EEA, UK, or similar jurisdictions may have rights relating to their Personal Data, including rights to:

- access Personal Data;
- request correction of inaccurate information;
- request deletion of Personal Data;
- request restriction of processing;
- object to certain processing activities;
- request portability of certain information;
- withdraw consent where processing is based on consent;
- request information regarding international transfers;
- lodge complaints with supervisory authorities.

Additional details regarding privacy rights are described in the “Your Privacy Rights” section of this Privacy Policy.

12.2 Lawful Processing and Legal Bases

Seneka processes Personal Data only where a lawful basis exists under applicable law.

Depending on the circumstances, processing may be based on:

- contractual necessity;
- legitimate interests;
- consent;
- legal obligations;
- protection of rights and security;

- compliance with applicable law.

Additional details regarding legal bases are described in the “Legal Bases for Processing” section of this Privacy Policy.

12.3 International Transfers and Safeguards

Users understand that Personal Data may be transferred outside the EEA, UK, or other jurisdictions where necessary to operate the Platform and Services.

Where required by applicable law, Seneka may implement safeguards relating to international data transfers, including:

- Standard Contractual Clauses (“SCCs”);
- contractual protections;
- technical safeguards;
- organizational safeguards;
- access controls;
- data protection measures recognized under applicable law.

Additional details regarding international transfers are described in the “International Data Transfers” section of this Privacy Policy.

12.4 Right to Lodge a Complaint

Users located in the EEA, UK, or similar jurisdictions may have the right to lodge complaints with their local data protection authority or supervisory authority if they believe their Personal Data has been processed in violation of applicable law.

Users are encouraged to contact Seneka first so that we may attempt to resolve concerns directly where appropriate.

12.5 Automated Processing and AI Systems

Certain Services provided by Seneka may involve automated processing, AI-assisted analysis, machine learning systems, or algorithmic processing.

AI-generated outputs are intended to assist Users and may involve:

- automated analysis;
- generated reports;
- recommendations;
- classifications;
- predictive outputs;
- workflow automation.

Users acknowledge that:

- AI-generated outputs may contain inaccuracies or incomplete information;
- AI-generated results require independent human review;
- AI outputs should not be relied upon as legal advice or professional legal opinion;
- automated systems may produce varying outcomes.

Where required by applicable law, Seneka may implement safeguards relating to automated processing activities.

12.6 Data Protection Representatives (Future)

At this time, Seneka may not maintain a formally designated EU or UK data protection representative where not legally required.

If applicable legal requirements change or operational activities require such designation in the future, Seneka may appoint appropriate representatives or contacts in relevant jurisdictions.

Updated representative information, if applicable, may be provided in future revisions of this Privacy Policy.

12.7 Contact Information for Privacy Requests

Users located in the EEA, UK, or similar jurisdictions may contact Seneka using the contact information provided in Section 19 of this Privacy Policy.

Seneka may request reasonable verification information before responding to certain requests.

12.8 Supplemental Rights and Local Laws

Nothing in this Privacy Policy is intended to limit rights provided under applicable privacy or data protection laws.

Additional rights, disclosures, or protections may apply depending on the User's jurisdiction.

SECTION 13 — CHILDREN'S PRIVACY

Seneka is not intended for use by children.

The Platform and Services are designed for adults, businesses, professionals, entrepreneurs, attorneys, law firms, and individuals capable of entering legally binding agreements.

13.1 Age Restrictions

Seneka does not knowingly permit individuals under eighteen (18) years of age to create accounts, access certain Services, engage in Marketplace activities, purchase subscriptions, submit legal-related information, or use attorney-related functionality.

If local law permits certain digital services for individuals above a lower minimum age, access may still be restricted where appropriate based on the nature of the Services.

Certain Services involving:

- legal workflows;
- Marketplace interactions;
- attorney communications;
- business transactions;
- subscriptions;
- AI-generated legal-related analysis;

- trademark-related services;

may require Users to be at least eighteen (18) years old or the age of majority in their jurisdiction.

13.2 No Knowing Collection From Children

Seneka does not knowingly collect Personal Data from children under the age permitted by applicable law.

If Seneka becomes aware that Personal Data has been collected from a child in violation of applicable law, we may take reasonable steps to:

- delete the information;
- deactivate associated accounts;
- restrict access to the Services;
- comply with applicable legal obligations.

13.3 Parent or Guardian Requests

Parents or legal guardians who believe that a child may have provided Personal Data to Seneka may contact us using the contact information provided in this Privacy Policy.

Where appropriate and legally required, Seneka may:

- investigate the request;
- verify identity and authority;
- remove information;
- restrict associated accounts;
- take reasonable remedial measures.

13.4 Marketplace and Attorney-Related Services

The Marketplace, attorney-related functionality, Workspace tools, AI-assisted trademark analysis, and legal-related Services are not directed toward children.

Seneka does not knowingly facilitate attorney-client interactions involving minors through the Platform without appropriate legal authority or supervision where required by applicable law.

Users are responsible for ensuring that any information they provide through the Platform complies with applicable laws relating to minors and legal capacity.

13.5 Educational and Public Resources

Certain educational materials, Resources content, or publicly accessible informational content may be viewable by general audiences.

However, such access does not authorize minors to create accounts, submit Personal Data, engage in transactions, or use restricted Services.

13.6 International Considerations

Because privacy laws relating to minors vary by jurisdiction, Seneka may apply additional restrictions, verification measures, or safeguards where required under applicable law.

13.7 Removal Requests and Compliance

Where required by applicable law, Seneka may comply with lawful requests relating to the removal, deletion, restriction, or protection of information associated with minors.

Certain information may nevertheless be retained where necessary for:

- legal compliance;
- fraud prevention;
- security;
- dispute resolution;
- enforcement of agreements;
- protection of rights and safety.

SECTION 14 — AI & AUTOMATED DECISION-MAKING

Seneka may provide AI-powered tools, automated analysis systems, machine-learning functionality, recommendation systems, and algorithmic processing features as part of the Platform and Services.

This section explains important information regarding the use of AI Services and automated processing within Seneka.

14.1 AI-Assisted Functionality

Certain Services may include AI-assisted functionality designed to help Users with activities such as:

- trademark analysis;
- brand evaluation;
- risk assessment;
- classification assistance;
- report generation;
- search assistance;
- content summarization;
- workflow automation;
- recommendations and suggestions;
- Marketplace assistance;
- document organization;
- business intelligence;
- legal-related informational analysis.

AI Services may generate outputs based on prompts, uploaded materials, user interactions, publicly available information, third-party systems, or automated processing methods.

14.2 AI Outputs Are Informational Only

AI-generated outputs provided through Seneka are for informational and assistive purposes only.

AI-generated outputs may include:

- automated reports;

- recommendations;
- scores;
- classifications;
- summaries;
- rankings;
- predictive outputs;
- generated insights;
- automated suggestions.

Such outputs may contain:

- inaccuracies;
- omissions;
- incomplete information;
- outdated information;
- incorrect assumptions;
- inconsistent results;
- hallucinated or fabricated content;
- limitations inherent to AI systems.

Users should not rely solely on AI-generated outputs when making legal, trademark, commercial, financial, operational, or business decisions.

The Services are intended for informational, operational, business, and technology-assistance purposes only and are not a substitute for independent legal advice, legal review, or professional judgment.

14.3 Human Verification Required

All AI-generated outputs require independent human review and verification.

Users are solely responsible for:

- evaluating AI-generated information;
- reviewing recommendations and reports;
- verifying factual accuracy;
- validating legal or trademark-related conclusions;
- consulting qualified professionals where appropriate;
- determining whether AI-generated outputs are suitable for their intended use.

AI-generated analysis should not be treated as a substitute for professional judgment, legal review, or independent trademark clearance.

14.4 No Legal Advice

Seneka is not a law firm and does not provide legal advice.

AI-generated outputs, recommendations, scores, classifications, analyses, or reports do not constitute:

- legal advice;
- legal opinion;
- legal representation;
- trademark clearance opinion;
- professional legal services;
- attorney-client communications.

Use of the Platform or AI Services does not create an attorney-client relationship between Seneka and any User.

Any attorney-client relationship may exist solely between Users and independent Attorneys under separate agreements.

14.5 Automated Suggestions and Decision Support

Certain features of the Platform may involve automated suggestions, scoring systems, recommendation engines, ranking systems, predictive functionality, or algorithmic processing.

These systems are intended to assist Users and may influence:

- search results;
- report outputs;
- risk indicators;
- recommendations;
- workflow suggestions;
- Marketplace visibility;
- prioritization systems;
- user experience personalization.

Automated systems may evolve over time and may produce different outputs based on:

- available data;
- model updates;
- prompts;
- user interactions;

- infrastructure changes;
- algorithmic adjustments;
- third-party AI providers.

14.6 AI Providers and Infrastructure

Certain AI-related functionality may rely on third-party AI providers, cloud infrastructure providers, machine-learning systems, or automated processing technologies operated by external providers.

As part of providing AI Services, certain information may be processed through AI-related infrastructure, including:

- prompts;
- uploaded content;
- generated outputs;
- operational metadata;
- interaction telemetry.

Users should avoid submitting information they do not wish to be processed through AI-enabled systems.

14.7 Limitations of AI Systems

AI systems may have technical, factual, operational, legal, linguistic, contextual, or analytical limitations.

AI Services may:

- produce inconsistent results;
- fail to identify relevant risks;
- generate incomplete recommendations;
- misinterpret context;
- incorrectly classify information;
- omit relevant considerations;
- produce outputs that require correction or verification.

Seneka does not guarantee:

- accuracy;
- completeness;
- reliability;

- legal sufficiency;
- regulatory compliance;
- uninterrupted availability;
- suitability for any particular purpose.

14.8 User Responsibility

Users are solely responsible for:

- decisions made using AI-generated outputs;
- review and validation of generated information;
- compliance with applicable law;
- independent professional review where appropriate;
- legal, trademark, business, or commercial decisions based on AI-assisted analysis.

Users should seek qualified legal counsel or professional advice when appropriate.

14.9 AI Improvement and Operational Processing

Seneka may process AI-related interaction data, prompts, generated outputs, operational telemetry, and related metadata for purposes including:

- service functionality;
- debugging;
- fraud prevention;
- abuse detection;
- analytics;
- system monitoring;
- reliability;
- operational improvement;
- infrastructure optimization;
- platform security.

Where appropriate, Seneka may aggregate, anonymize, minimize, or de-identify certain operational information.

14.10 Evolving AI Technologies

AI technologies and regulatory requirements continue to evolve.

Seneka may modify, improve, replace, restrict, suspend, or update AI-related functionality, safeguards, or operational practices over time in response to:

- legal developments;
- technological changes;
- operational needs;
- infrastructure changes;
- safety considerations;
- regulatory guidance;
- industry standards.

SECTION 15 — MARKETPLACE & ATTORNEY DISCLAIMER

Seneka may provide Marketplace functionality, attorney discovery tools, professional profile features, communication systems, collaboration tools, referrals, informational resources, or other features designed to facilitate interactions between Users, Attorneys, law firms, service providers, and other Marketplace participants.

This section explains important limitations relating to such functionality.

15.1 Seneka Is Not a Law Firm

Seneka is a technology platform and is not a law firm, legal practice, legal referral service, or legal representation provider.

Seneka does not provide:

- legal advice;
- legal opinions;
- legal representation;
- trademark clearance opinions;
- legal strategy;
- attorney services;
- legal filings;

- legal certifications;
- legal guarantees.

Any information, reports, recommendations, AI-generated outputs, Marketplace content, or communications provided through the Platform are for informational and technology-assistance purposes only.

15.2 Attorneys and Professionals Are Independent

Attorneys, law firms, trademark professionals, consultants, and other Marketplace participants are independent third parties and are not employees, agents, partners, joint venturers, representatives, or affiliates of Seneka solely by virtue of using the Platform.

Seneka does not control or direct:

- legal services;
- legal advice;
- attorney conduct;
- professional judgment;
- communications between Users;
- legal filings;
- legal outcomes;
- client representation;
- professional obligations.

Any professional relationship exists solely between Users and the independent Attorney or professional engaged through or outside the Platform.

15.3 No Attorney-Client Relationship With Seneka

Use of the Platform, AI Services, Marketplace features, messaging systems, public resources, attorney discovery tools, or communications through Seneka does not create an attorney-client relationship between Seneka and any User.

An attorney-client relationship may only arise between a User and an independent Attorney under a separate agreement outside the scope of this Privacy Policy.

Users are solely responsible for determining whether to engage an Attorney or professional.

15.4 No Endorsement or Certification

Seneka does not endorse, certify, recommend, guarantee, verify, warrant, or assure:

- the qualifications of Attorneys;
- professional licenses;
- legal competence;
- professional standing;
- legal advice;
- legal outcomes;
- Marketplace content;
- user-generated reviews;
- ratings or recommendations;
- AI-generated suggestions;
- business or trademark success.

Profiles, reviews, rankings, badges, ratings, recommendations, or Marketplace visibility may be generated through automated systems, user submissions, third-party information, operational metrics, or other processes.

Marketplace placement or visibility does not constitute endorsement by Seneka.

15.5 No Guarantees or Warranties

Seneka does not guarantee:

- trademark registration outcomes;
- legal success;
- business outcomes;
- Marketplace results;
- attorney availability;
- attorney responsiveness;
- professional qualifications;
- legal accuracy;
- uninterrupted Services;
- successful filings;
- conflict-free trademark results;
- regulatory compliance.

Users acknowledge that legal, trademark, and business matters inherently involve uncertainty and risk.

15.6 User Responsibility and Independent Judgment

Users are solely responsible for:

- evaluating Attorneys and professionals;
- verifying credentials and qualifications;
- reviewing legal advice;
- making trademark or business decisions;
- reviewing agreements;
- conducting independent due diligence;
- determining suitability of professional services;
- evaluating AI-generated outputs and recommendations.

Users should seek independent professional advice where appropriate.

15.7 No Responsibility for Legal Services

To the fullest extent permitted by applicable law, Seneka is not responsible or liable for:

- legal advice;
- professional services;
- legal representation;
- attorney conduct;
- missed deadlines;
- filings;
- communications between Users;
- disputes between Users and Attorneys;
- malpractice claims;
- professional negligence;
- legal outcomes;
- business losses;
- trademark disputes;
- user reliance on Marketplace content;
- actions or omissions of independent professionals.

Any disputes regarding legal services or professional conduct must be resolved directly between the relevant parties.

15.8 Platform Intermediary Functionality

Seneka acts solely as a technology platform and intermediary provider that may facilitate:

- communication tools;
- attorney discovery;
- Marketplace functionality;
- AI-assisted workflows;
- collaboration systems;
- informational resources;
- payment processing support;
- document organization;
- Workspace management.

Seneka does not act as:

- an agent;
- fiduciary;
- legal representative;
- partner;
- employer;
- guarantor;
- broker of legal services.

15.9 Marketplace Communications and User Content

Communications, documents, recommendations, reviews, ratings, messages, uploaded materials, and Marketplace interactions may originate from Users, Attorneys, or third parties.

Seneka does not independently verify all Marketplace content or communications and is not responsible for the accuracy, completeness, legality, reliability, or appropriateness of such content.

Users are responsible for evaluating information shared through the Marketplace.

15.10 Jurisdictional and Regulatory Considerations

Legal services regulations vary by jurisdiction.

Certain Marketplace functionality may be unavailable, restricted, or modified depending on applicable laws, licensing rules, ethical obligations, or operational requirements.

Users are responsible for complying with laws applicable to their jurisdiction and professional activities.

15.11 AI-Assisted Marketplace Features

Certain Marketplace or attorney-related functionality may involve AI-assisted recommendations, automated ranking systems, generated insights, or algorithmic suggestions.

Such systems may:

- produce incomplete or inaccurate recommendations;
- rely on automated processing;
- evolve over time;
- generate varying results.

AI-assisted functionality does not replace independent legal judgment, attorney review, or professional due diligence.

SECTION 16 — PUBLIC SHARING FEATURES

Certain Services provided by Seneka may allow Users to voluntarily create, publish, generate, or share public-facing content, including public reports, share pages, public brand cards, scorecards, summaries, social sharing links, or other publicly accessible materials.

This section explains how public sharing functionality operates and the privacy implications associated with publicly shared content.

16.1 Voluntary Public Sharing

Seneka may provide features enabling Users to voluntarily make certain information publicly accessible.

Such features may include:

- public brand cards;
- public share pages;
- shareable URLs;
- public scorecards;
- report previews;
- SEO-oriented public pages;
- social sharing functionality;
- public profile elements;
- generated public summaries;
- publicly accessible brand-related content.

Users are solely responsible for determining what information they choose to make publicly available.

16.2 Public Accessibility and Visibility

Content intentionally shared through public sharing functionality may become publicly accessible and viewable by:

- other Users;
- website visitors;
- third parties;
- search engines;
- social media platforms;
- analytics systems;
- indexing technologies;
- automated crawlers;
- AI systems operated by third parties.

Publicly shared information may potentially be copied, reposted, archived, indexed, cached, screenshotted, redistributed, or referenced by third parties outside Seneka’s control.

16.3 Search Engines and Indexed Content

Public pages or publicly accessible URLs may be indexed by search engines and discoverable through online search results.

This may include indexing by:

- search engines;
- social platforms;
- web crawlers;
- AI indexing systems;
- content discovery technologies;
- automated retrieval systems.

Even after removal or deletion, cached or archived versions of publicly accessible content may remain temporarily available through third-party systems beyond Seneka's control.

16.4 Social Sharing and External Platforms

Users may voluntarily share public links, reports, scorecards, summaries, or public pages through external platforms, including:

- social media services;
- messaging applications;
- professional networks;
- forums;
- email communications;
- external websites.

Once content is shared externally, Seneka cannot control:

- third-party redistribution;
- reposting;
- public visibility;
- indexing;
- external storage;
- audience access;
- platform-specific privacy settings.

Use of external platforms is subject to the privacy policies and practices of those third parties.

16.5 Public Brand Cards and Generated Summaries

Certain Services may generate public-facing brand cards, scorecards, previews, rankings, summaries, or AI-generated informational content intended for sharing or visibility purposes.

Such content may include:

- proposed brand names;
- risk indicators;
- AI-generated summaries;
- scores or ratings;
- public descriptions;
- visual branding elements;
- shared report excerpts;
- publicly generated metadata.

Users are responsible for reviewing publicly shared content before publication or distribution.

16.6 User Control Over Sharing

Where functionality permits, Users may have the ability to:

- create public pages;
- disable public sharing;
- delete public links;
- restrict visibility;
- modify shared content;
- remove publicly accessible materials.

However, removal from the Platform does not guarantee removal from:

- search engine caches;
- third-party archives;
- screenshots;
- reposted copies;
- automated indexing systems;
- external websites.

16.7 Visibility and Confidentiality Risks

Users should carefully evaluate whether they wish to publicly share:

- trademarks;
- proposed business names;
- legal-related information;
- Marketplace interactions;
- business strategies;
- confidential information;
- commercially sensitive materials;
- Workspace content;
- AI-generated reports.

Public disclosure of certain information may create:

- confidentiality risks;
- reputational risks;
- intellectual property risks;
- trademark-related risks;
- commercial visibility risks;
- indexing exposure;
- unauthorized redistribution risks.

Users are solely responsible for assessing such risks before enabling public sharing functionality.

16.8 No Confidentiality for Public Content

Information intentionally made public through sharing functionality may no longer be considered confidential.

Seneka cannot guarantee confidentiality, removal from third-party systems, or restricted access to publicly shared materials once publicly distributed or indexed.

16.9 Public Analytics and Engagement Metrics

Seneka may collect operational information relating to public sharing functionality, including:

- link engagement;

- page views;
- traffic metrics;
- sharing activity;
- interaction statistics;
- public engagement analytics.

Such information may be used for:

- analytics;
- product improvement;
- feature optimization;
- operational monitoring;
- fraud prevention;
- service reliability.

16.10 AI and Automated Indexing Systems

Publicly accessible content may potentially be accessed, indexed, processed, summarized, or analyzed by AI systems, automated retrieval systems, search technologies, or third-party machine learning systems outside Seneka's control.

Seneka does not control how third parties process publicly available information once it has been publicly shared.

SECTION 17 — THIRD-PARTY LINKS & SERVICES

The Platform and Services may contain links to third-party websites, services, platforms, APIs, integrations, applications, tools, resources, or external content that are not owned, operated, or controlled by Seneka.

This section explains how third-party services may interact with the Platform and the limitations of Seneka's responsibility regarding such services.

17.1 Third-Party Services and Integrations

Seneka may use, integrate with, rely upon, or provide access to third-party services relating to:

- payment processing;
- subscription management;
- AI and machine learning functionality;
- analytics and monitoring;
- communications;
- customer support;
- authentication;
- cloud infrastructure;
- Marketplace functionality;
- document processing;
- APIs and developer tools;
- hosting and content delivery;
- operational tooling;
- attorney-related services;
- external business resources.

Third-party services may be integrated directly into the Platform or accessed through links, APIs, embedded content, workflows, or external systems.

17.2 External Websites and Links

The Platform may contain links to external websites, resources, attorney websites, law firm pages, social media platforms, public databases, business tools, educational resources, or third-party services.

Such links are provided solely for convenience, informational purposes, or Marketplace functionality.

Seneka does not control and is not responsible for:

- external websites;
- third-party content;
- third-party availability;
- third-party security practices;
- privacy practices of external services;
- third-party policies;
- external business practices;

- legal services provided by third parties;
- information accuracy on external platforms.

Accessing third-party services occurs at the User’s own risk.

17.3 Payment Providers and Subscription Platforms

Certain paid Services may rely on third-party payment processors, subscription providers, app marketplaces, or billing infrastructure providers.

Such providers may include:

- Stripe;
- Paddle;
- RevenueCat;
- Apple App Store;
- Google Play;
- other authorized payment or subscription providers.

Payment transactions, billing operations, and subscription processing may be governed by the privacy policies and terms of those third parties.

Seneka does not control the independent practices of payment providers or app marketplace operators.

17.4 AI Providers and Automated Processing Services

Certain AI-related functionality may rely on third-party AI providers, machine-learning systems, APIs, cloud providers, or automated processing infrastructure.

Such providers may include:

- OpenAI;
- cloud AI infrastructure providers;
- machine-learning APIs;
- language model providers;
- AI processing systems;
- inference infrastructure providers.

Information submitted through AI-enabled features may be processed by third-party AI systems where necessary to provide AI functionality.

Users should avoid submitting information they do not wish to be processed through third-party AI systems.

Seneka does not guarantee the accuracy, reliability, legality, completeness, or suitability of outputs generated by third-party AI systems.

17.5 Marketplace and Attorney Websites

Marketplace functionality may allow Users to access or interact with:

- attorney websites;
- law firm websites;
- booking systems;
- professional profiles;
- external communication systems;
- scheduling platforms;
- legal service providers.

Seneka does not control the independent operations, legal compliance, professional conduct, privacy practices, or security measures of Attorneys, law firms, or external professional services.

Any relationship established between Users and third-party professionals exists independently of Seneka.

17.6 APIs, Developer Tools, and External Systems

Certain Services may involve APIs, integrations, developer tools, embedded systems, or external platforms.

Use of such functionality may involve transmission or processing of information between Seneka and third-party systems.

Third-party APIs or integrations may:

- collect information independently;
- apply separate privacy practices;

- maintain separate terms;
- process information outside Seneka's control;
- introduce operational or security risks.

Users are responsible for reviewing applicable third-party terms and privacy practices before using integrated services.

17.7 No Endorsement of Third Parties

References to third-party providers, Attorneys, integrations, services, APIs, products, websites, or external resources do not constitute:

- endorsement;
- sponsorship;
- certification;
- recommendation;
- guarantee;
- partnership;
- representation;
- approval by Seneka.

Marketplace visibility, integrations, rankings, or references may result from automated systems, user interactions, technical functionality, or operational considerations.

17.8 Third-Party Responsibility Limitations

To the fullest extent permitted by applicable law, Seneka is not responsible or liable for:

- acts or omissions of third parties;
- third-party privacy practices;
- third-party data handling;
- external websites;
- third-party AI outputs;
- external integrations;
- attorney conduct;
- third-party security incidents;
- payment processor failures;
- external platform availability;
- API interruptions;

- content hosted outside Seneka’s systems;
- external legal services;
- losses arising from use of third-party services.

Users acknowledge that use of third-party services may involve separate risks, obligations, and legal relationships.

17.9 Third-Party Terms and Policies

Third-party services accessible through the Platform may be governed by separate:

- privacy policies;
- terms of service;
- subscription agreements;
- API terms;
- professional agreements;
- billing policies;
- security practices.

Users are responsible for reviewing and understanding such third-party terms before interacting with external services.

17.10 Evolving Integrations and External Services

Seneka may add, modify, suspend, replace, or discontinue third-party integrations, APIs, providers, or external services over time.

Availability of integrations and external functionality may vary depending on:

- jurisdiction;
- operational requirements;
- provider availability;
- legal restrictions;
- technical limitations;
- business considerations.

SECTION 18 — CHANGES TO THIS PRIVACY POLICY

Seneka may update, modify, revise, replace, or supplement this Privacy Policy from time to time to reflect changes in:

- the Platform or Services;
- legal or regulatory requirements;
- AI technologies;
- Marketplace functionality;
- operational practices;
- data processing activities;
- security practices;
- integrations or third-party providers;
- business operations;
- industry standards.

18.1 Effective Date and Latest Revision

The “Last Updated” or similar date displayed at the beginning of this Privacy Policy indicates the effective date of the most recent revision.

Updated versions of this Privacy Policy become effective as of the published revision date unless otherwise stated.

Users are encouraged to periodically review this Privacy Policy to remain informed about Seneka’s data practices and privacy-related updates.

18.2 Notice of Material Changes

Where required by applicable law or where changes are considered material, Seneka may provide notice through one or more methods, including:

- posting updated policies on the Platform;
- account notifications;
- email communications;
- Workspace notices;
- application alerts;
- website banners;
- Marketplace notifications;

- operational announcements;
- other reasonable communication methods.

The method and timing of notifications may vary depending on:

- the nature of the changes;
- legal obligations;
- operational considerations;
- technical capabilities;
- User settings.

18.3 Continued Use of the Services

By continuing to access or use the Platform or Services after an updated Privacy Policy becomes effective, Users acknowledge and understand that the revised Privacy Policy applies to their continued use of the Services, to the extent permitted by applicable law.

If a User does not agree with the updated Privacy Policy, the User should discontinue use of the Services and may request account deletion where applicable.

18.4 Legal and Regulatory Compliance Updates

Certain updates to this Privacy Policy may be necessary to comply with:

- privacy laws;
- data protection regulations;
- AI-related regulations;
- consumer protection laws;
- Marketplace requirements;
- payment provider requirements;
- app marketplace policies;
- security obligations;
- operational or infrastructure changes.

Seneka reserves the right to implement such changes as necessary to maintain compliance and operational integrity.

18.5 Historical Versions

Seneka may maintain historical or archived versions of this Privacy Policy for legal, operational, compliance, auditing, or recordkeeping purposes.

Archived versions may not always remain publicly accessible.

18.6 No Waiver of Rights

Failure by Seneka to enforce any provision, right, safeguard, or policy described in this Privacy Policy shall not constitute a waiver of such rights or protections.

SECTION 19 — CONTACT INFORMATION

If you have questions, concerns, requests, or complaints regarding this Privacy Policy, the Platform, Personal Data processing activities, privacy practices, AI-related processing, Marketplace functionality, or applicable privacy rights, you may contact Seneka using the information below.

19.1 Legal Entity

The Platform and Services are operated by:

Seneka

Legal Entity:

LUKAS INNOVATION GROUP LLC

Jurisdiction:

Wyoming, United States

Registered Address:

312 WEST 2ND ST UNIT A9449

Casper, WY 82609

United States

Additional operational, billing, or legal contact information may be provided through the Platform or official communications.

19.2 General Contact Information

General inquiries regarding the Platform or Services may be directed to:

General Contact Email:
support@senekalegal.com

Support Email:
support@senekalegal.com

19.3 Privacy and Data Protection Requests

Privacy-related requests, including requests relating to:

- access;
- deletion;
- correction;
- portability;
- restriction;
- objections;
- consent withdrawal;
- California privacy rights;
- GDPR-related requests;
- data protection concerns;
- AI-related privacy concerns;

may be directed to:

Privacy Contact Email:
privacy@senekalegal.com

Seneka may request reasonable identity verification information before processing certain requests.

19.4 GDPR / UK GDPR Contact

Users located in the European Economic Area (“EEA”), United Kingdom (“UK”), Switzerland, or similar jurisdictions may contact Seneka regarding:

- GDPR-related requests;
- international transfers;
- automated processing concerns;
- AI-related processing questions;
- data protection concerns;
- supervisory authority matters.

GDPR Contact Email:
privacy@senekalegal.com

Where required by applicable law, additional regional contact details or representative information may be provided in future updates to this Privacy Policy.

19.5 Future Data Protection Officer or Representatives

At this time, Seneka may not maintain a formally designated:

- Data Protection Officer (“DPO”);
- EU Representative;
- UK Representative;

where not legally required.

If applicable laws, operational activities, enterprise requirements, or regulatory obligations require such appointments in the future, Seneka may designate appropriate representatives or officers.

Updated representative information may be published in future revisions of this Privacy Policy.

19.6 Response Timing and Verification

Seneka will seek to respond to legitimate privacy-related inquiries and verified requests within commercially reasonable timeframes and as required under applicable law.

To protect Users and maintain security, Seneka may:

- verify identity;
- request additional documentation;
- authenticate account ownership;
- decline requests where legally permitted;
- limit abusive or excessive requests.

19.7 Regulatory Authorities

Users may also have the right to contact applicable supervisory authorities, regulators, consumer protection agencies, or data protection authorities in their jurisdiction if they believe their Personal Data has been processed in violation of applicable law.

Where appropriate, Users are encouraged to contact Seneka first so that we may attempt to address concerns directly.

19.8 Official Communications

Privacy-related notices, legal notices, operational communications, Marketplace notifications, and policy updates may be delivered through:

- email;
- account notifications;
- Workspace alerts;
- website notices;
- mobile application notices;
- Platform messaging systems;
- other reasonable communication methods.

Users are responsible for maintaining accurate contact information associated with their accounts.

SECTION 20 — U.S. STATE PRIVACY ADDENDUM

This U.S. State Privacy Addendum supplements the other sections of this Privacy Policy and applies to residents of U.S. states that provide applicable consumer privacy rights under state privacy laws.

As privacy laws in the United States continue to evolve, Seneka may update this section to reflect additional legal obligations, consumer rights, operational requirements, or jurisdiction-specific disclosures.

This section is intended to support compliance with applicable U.S. state privacy laws, including laws enacted in jurisdictions such as:

- California;
- Virginia;
- Colorado;
- Connecticut;
- Utah;
- and other U.S. states adopting privacy or consumer data protection legislation.

20.1 Scope of State Privacy Rights

Depending on the User's state of residence and applicable law, Users may have certain rights relating to Personal Data, including rights to:

- access information;
- correct inaccurate information;
- request deletion;
- obtain portability of certain information;
- opt out of certain targeted advertising activities;
- opt out of certain profiling activities;
- opt out of certain data sharing activities;
- limit certain uses of sensitive information;
- appeal certain privacy-related decisions;
- receive disclosures regarding data practices.

Availability of rights may vary depending on:

- applicable law;
- jurisdiction;
- nature of the processing;
- business or commercial exemptions;

- operational limitations;
- legal exceptions.

20.2 Categories of Personal Data

The categories of Personal Data Seneka may collect, process, disclose, retain, or use are described throughout this Privacy Policy and may include:

- identifiers;
- account information;
- billing information;
- Marketplace data;
- Workspace content;
- AI interaction data;
- device and technical information;
- analytics information;
- uploaded materials;
- communications;
- generated reports;
- operational telemetry;
- business-related information;
- inferred insights.

Additional information regarding categories of Personal Data is described in the “California Privacy Notice” and other sections of this Privacy Policy.

20.3 Purposes of Processing

Seneka may process Personal Data for purposes including:

- providing Services;
- account management;
- authentication and security;
- fraud prevention;
- Marketplace functionality;
- AI-assisted analysis;
- trademark and brand-related analysis;
- analytics and diagnostics;
- subscription management;
- operational improvement;
- legal compliance;

- customer support;
- infrastructure maintenance;
- protection of rights and security.

Additional details regarding processing purposes are described throughout this Privacy Policy.

20.4 Sensitive Information

Depending on the Services used and applicable law, certain information processed by Seneka may be considered sensitive information under state privacy laws.

Such information may include:

- account credentials;
- authentication-related information;
- uploaded materials;
- business-sensitive content;
- communications;
- Marketplace interactions.

Seneka seeks to process sensitive information only as reasonably necessary to provide the Services, maintain security, comply with law, support operational functionality, or protect rights and integrity of the Platform.

20.5 Targeted Advertising and Profiling

Certain analytics, personalization, operational, recommendation, or advertising-related activities may be considered targeted advertising or profiling under applicable state privacy laws.

Where required by law, Users may have rights to opt out of certain targeted advertising or profiling activities.

Seneka may implement additional mechanisms, disclosures, or controls where legally required.

At this time, Seneka does not sell Personal Data in exchange for monetary compensation.

20.6 Appeals Process

Where required under applicable state privacy laws, Users may have the right to appeal certain decisions relating to privacy requests.

Information regarding applicable appeals procedures may be provided upon denial of a privacy request where required by law.

20.7 Verification of Requests

To protect privacy, security, and account integrity, Seneka may:

- verify identity;
- authenticate account ownership;
- request supporting information;
- decline fraudulent or abusive requests;
- limit repetitive or excessive requests where permitted by law.

Authorized agents acting on behalf of Users may be required to provide documentation demonstrating authority to act on behalf of the User.

20.8 No Sale of Personal Data

Seneka does not sell Personal Data in exchange for monetary compensation.

Certain disclosures to analytics providers, infrastructure providers, operational vendors, AI providers, or service providers may constitute “sharing” under certain state privacy laws depending on applicable legal interpretation.

Such disclosures are made for operational, security, service-related, analytics, infrastructure, or business purposes.

20.9 Future State-Specific Disclosures

As additional U.S. states adopt privacy laws or regulations, Seneka may provide:

- supplemental disclosures;
- additional consumer rights notices;

- opt-out mechanisms;
- jurisdiction-specific notices;
- updated privacy controls;
- enhanced transparency measures.

Updated state-specific disclosures may be incorporated into future revisions of this Privacy Policy.

20.10 AI, Profiling, and Automated Processing

Certain Services may involve:

- AI-assisted analysis;
- automated processing;
- recommendation systems;
- predictive outputs;
- profiling;
- workflow automation;
- automated suggestions.

Where required by applicable law, Seneka may provide additional disclosures, safeguards, or controls relating to automated processing or profiling activities.

AI-generated outputs require independent human review and should not be treated as legal advice or professional legal opinions.

FINAL SECTION — CONCLUSION / ACKNOWLEDGMENT

21. Final Provisions

Seneka is committed to maintaining a privacy-conscious, security-focused, and transparent approach to the operation of the Platform and Services.

We recognize that privacy, security, AI governance, data protection, and responsible handling of information are important to our Users, including businesses, entrepreneurs, professionals, attorneys, law firms, and Marketplace participants.

Seneka continually seeks to improve:

- privacy practices;
- security safeguards;
- operational transparency;
- AI-related protections;
- compliance procedures;
- user controls;
- platform integrity;
- responsible data handling practices.

By accessing or using the Platform or Services, Users acknowledge that they have reviewed and understood this Privacy Policy and understand that certain processing, storage, sharing, AI-assisted functionality, Marketplace interactions, and international transfers may occur as described herein.

If Users do not agree with this Privacy Policy or applicable data practices, they should discontinue use of the Platform and Services.

Nothing in this Privacy Policy is intended to limit any non-waivable rights provided under applicable law.
