
SCIREAT LLC

Privacy Policy

Effective Date: September 13, 2026 | **Version:** v2.0 | **Jurisdiction of**

Organization: Kansas, United States

Principal Place of Business: Maize, Kansas, United States

Privacy Officer Contact: privacy@scireat.com | **DPO Contact (GDPR):**
dpo@scireat.com

Table of Contents

1. Introduction and Scope

2. Definitions

3. Information We Collect

3.1 Information You Provide Directly | 3.2 Information Collected Automatically | 3.3
Information from Third Parties

3.4 Health-Financial Intersection Data | 3.5 IncomeCompliant-Specific Data | 3.6 Accelavest
Financial Services Data | 3.7 Sensitive Personal Information

4. Purposes and Legal Bases for Processing

4.1–4.7 Service Delivery, Legal Compliance, Fraud Prevention, Analytics, Marketing, GDPR
Bases, GLBA

5. HIPAA-Adjacent Protections for Health-Financial Data

5.1–5.9 Scope, Minimum Necessary, Permitted Uses, BAAs, De-Identification, Individual
Rights, Security, FTC Rule, State Laws

6. How We Share Your Information

6.1–6.8 Intra-Group, Service Providers, Financial Institutions, Business Associates, Legal, Business Transfers, Consent, CCPA Table

7. SaaS-Specific Provisions — IncomeCompliant

7.1–7.8 Architecture, Customer Data, DPAs, Subprocessors, Portability, Deletion, SLAs, Automated Decisions

8. Cookies and Tracking Technologies

9. Data Retention

10. Data Security

11. International Data Transfers

12. Your Rights and Choices

12.1 U.S. Federal Law | 12.2 Kansas Residents | 12.3 California Residents (CCPA/CPRA) | 12.4 EEA and UK Residents (GDPR) | 12.5 How to Exercise Your Rights

13. Children's Privacy

14. Third-Party Links and Integrations

15. Changes to This Privacy Policy

16. Contact Information and Data Controller Details

17. Regulatory Compliance Summary Table

1. INTRODUCTION AND SCOPE

1.1 Who We Are

Scireat LLC is a limited liability company organized and existing under the laws of the State of Kansas, United States, with its principal place of business in Maize, Kansas. Scireat LLC serves as the parent holding company of a group of wholly-owned subsidiaries, collectively referred to throughout this Privacy Policy as the

"Scireat Group" or, as the context permits, **"we," "us,"** or **"our."** The Scireat Group presently comprises the following entities:

- **Scireat LLC** — Parent holding company, organized under the laws of Kansas, United States;
- **Sciorbis Business Group LLC** — Wholly-owned subsidiary providing business services;
- **Accelavest Financial Services LLC** — Wholly-owned subsidiary providing investment advisory and financial planning services, subject to applicable financial regulatory requirements including the Gramm-Leach-Bliley Act (GLBA); and
- **Mersellus LLC** — Wholly-owned subsidiary engaged in operations as designated by Scireat LLC management.

Each of the foregoing entities is a party to and bound by this Privacy Policy. Where provisions of this Privacy Policy apply specifically to a single entity, such entity is named expressly.

1.2 What This Policy Covers

This Privacy Policy describes the categories of personal information and data that the Scireat Group collects, the purposes for which such information is collected and processed, the legal bases upon which processing rests, the circumstances under which information may be disclosed to third parties, and the rights that individuals have with respect to their personal information. This Privacy Policy applies to:

- All websites, subdomains, and web applications owned or operated by any member of the Scireat Group, including but not limited to scireat.com and its subdomains;
- All mobile applications published by any member of the Scireat Group;
- The **IncomeCompliant** cloud-based financial compliance and income-tracking SaaS platform and all features, modules, and APIs associated therewith;

- All services, products, and operations conducted by Sciorbis Business Group LLC, Accelavest Financial Services LLC, and Mersellus LLC, except to the extent a subsidiary has issued a separate, subsidiary-specific privacy notice that expressly supplements or modifies this Policy with respect to defined activities; and
- Any other interaction between an individual and any member of the Scireat Group, whether online, by telephone, by electronic communication, or in person, to the extent personal information is collected in the course of such interaction.

1.3 Relationship Between This Policy and Subsidiary-Level Notices

This Privacy Policy constitutes the overarching group-level privacy governance instrument for the Scireat Group. Individual subsidiaries may issue supplemental privacy notices that address activities, data categories, or regulatory requirements specific to their business operations. Where a subsidiary-specific notice exists, it applies in addition to and not in derogation of this Policy. In the event of a direct conflict between a subsidiary-specific notice and this Privacy Policy on a matter of individual data rights, the provision affording greater protection to the individual shall govern. Scireat LLC maintains a registry of subsidiary-level notices, available upon request to privacy@scireat.com.

1.4 HIPAA Applicability Statement

This Privacy Policy is **not** a Notice of Privacy Practices as required under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 45 C.F.R. Parts 160 and 164. Members of the Scireat Group do not function as Covered Entities under HIPAA in all contexts in which they operate. Nonetheless, because the IncomeCompliant platform and certain Accelavest Financial Services operations may involve data that intersects health plan administration, health insurance enrollment, HSA and FSA account management, and health-plan-linked income or benefit determinations, the Scireat Group voluntarily applies HIPAA-equivalent privacy and security standards — including the Minimum Necessary standard, Business Associate Agreement protocols, and de-identification procedures — to all such health-financial data, as described in detail in Section 5 of this Privacy Policy.

Where the Scireat Group does act as a Business Associate of a Covered Entity by virtue of a contractual relationship and the scope of services rendered, the terms of the applicable Business Associate Agreement (BAA) shall govern the processing of Protected Health Information, and the provisions of this Policy shall apply to all other personal information processed in connection with that relationship.

2. DEFINITIONS

For purposes of this Privacy Policy, the following terms shall have the meanings set forth below. Terms not defined herein shall be interpreted consistently with their definitions under applicable law, including without limitation HIPAA, GLBA, the California Consumer Privacy Act as amended by the California Privacy Rights Act (CCPA/CPRA), and the General Data Protection Regulation (GDPR).

"Authorized User" means an individual who has been granted access credentials by an enterprise customer of the IncomeCompliant platform and who accesses the platform pursuant to the enterprise customer's subscription agreement with Scireat LLC.

"Business Associate" has the meaning set forth in 45 C.F.R. § 160.103, and refers to a person or entity that performs certain functions or activities on behalf of, or provides certain services to, a Covered Entity that involve the use or disclosure of Protected Health Information. For purposes of this Privacy Policy, when the Scireat Group acts in such capacity, the applicable BAA governs PHI processing.

"Consumer" means a natural person who is a resident of a state that has enacted a consumer privacy law under which that term is defined, including a California resident as defined by the CCPA/CPRA. Where the context does not implicate a specific statutory definition, "Consumer" refers broadly to any natural person whose Personal Data is processed by the Scireat Group.

"Covered Entity" has the meaning set forth in 45 C.F.R. § 160.103, and refers to a health plan, health care clearinghouse, or health care provider who transmits any health information in electronic form in connection with a transaction covered under HIPAA.

"Data Breach" means any unauthorized acquisition, access, use, or disclosure of Personal Data maintained by the Scireat Group that compromises the security, confidentiality, or integrity of such information, as further defined under applicable state and federal breach notification laws.

"Data Controller" means the natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of Personal Data. Scireat LLC is the Data Controller with respect to Personal Data processed in connection with its own operations and those of the Scireat Group, except where Scireat LLC acts as a Data Processor on behalf of an enterprise customer.

"Data Processor" means a natural or legal person, public authority, agency, or other body that processes Personal Data on behalf of the Data Controller. When Scireat LLC provides the IncomeCompliant platform to enterprise customers, Scireat LLC acts as Data Processor with respect to Customer Data uploaded to or generated through the platform by or on behalf of the enterprise customer.

"De-identification" means the process by which Personal Data or Protected Health Information is altered so that it no longer identifies or can be reasonably used to identify an individual, either through the Safe Harbor method under 45 C.F.R. § 164.514(b)(2) (removal of 18 specified HIPAA identifiers) or through the Expert Determination method under 45 C.F.R. § 164.514(b)(1) (statistical verification by a qualified expert).

"Electronic Protected Health Information" or "ePHI" means Protected Health Information that is created, received, maintained, or transmitted in electronic form, as defined under 45 C.F.R. § 160.103.

"Health-Financial Data" means data that simultaneously implicates an individual's health or health plan enrollment status and that individual's financial information, income, or benefit eligibility, including but not limited to: insurance premium payment records linked to health plan identifiers, HSA and FSA contribution and distribution data, health-plan-linked income determinations, Medicaid and CHIP eligibility records, and employer-sponsored health benefit enrollment data linked to

payroll or income records. Health-Financial Data may constitute PHI, ePHI, or quasi-PHI depending on context, and in all cases is subject to the heightened protections described in Section 5.

"IncomeCompliant Platform" means the cloud-based financial compliance and income-tracking software-as-a-service platform developed, operated, and maintained by Scireat LLC, accessible at the URLs designated by Scireat LLC from time to time, and all associated APIs, integrations, mobile applications, and support services.

"Personal Data" or "Personal Information" means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to an identified or identifiable natural person. This includes, without limitation, name, postal address, email address, telephone number, Social Security number, financial account information, government-issued identification numbers, biometric data, geolocation data, and Internet or other electronic network activity information.

"Processing" means any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

"Protected Health Information" or "PHI" has the meaning set forth in 45 C.F.R. § 160.103, and means individually identifiable health information that is created or received by a Covered Entity or Business Associate and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual, and that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

"Pseudonymization" means the processing of Personal Data in such a manner that the data can no longer be attributed to a specific individual without the use of

additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the Personal Data is not attributed to an identified or identifiable natural person.

"Scireat Group" means, collectively, Scireat LLC, Sciorbis Business Group LLC, Accelavest Financial Services LLC, and Mersellus LLC, and any future wholly-owned subsidiaries added to the group, as updated on the Scireat LLC website from time to time.

"Sensitive Personal Information" means a subset of Personal Data that warrants heightened protection by virtue of the particular sensitivity of the information or the harm that could result from its unauthorized disclosure, including: Social Security numbers and other government-issued identification numbers; financial account numbers, debit and credit card numbers, and associated access credentials; precise geolocation data; racial or ethnic origin; religious or philosophical beliefs; union membership; genetic data; biometric data processed for the purpose of uniquely identifying a natural person; data concerning health; data concerning a natural person's sex life or sexual orientation; the contents of an individual's mail, email, or text messages; and health plan identifiers linked to an individual.

"User" means any natural person who accesses or uses any Scireat Group website, application, or service, whether as a registered account holder, Authorized User of the IncomeCompliant platform, or as an unregistered visitor.

3. INFORMATION WE COLLECT

The Scireat Group collects Personal Data through multiple channels and from multiple sources. The categories of Personal Data we collect, and the sources from which we collect them, are described below. Not all categories of data described in this Section are collected in every context; the specific data collected depends on the nature of the Scireat Group service or product with which the individual is interacting.

3.1 Information You Provide Directly

We collect Personal Data that individuals voluntarily provide to us in the course of interacting with our services, including:

- **Account Registration:** First and last name, business name or employer name, email address, postal address, telephone number, username, password (stored in hashed, salted form), and account preferences provided when creating an account on any Scireat Group platform;
- **Contact and Support Requests:** The content of messages, attachments, and communications submitted through contact forms, support ticket systems, email correspondence, or telephone calls, including any Personal Data included in such communications;
- **Subscription and Billing Data:** Payment card information (processed by our PCI DSS-compliant payment processor; Scireat does not store full payment card numbers), billing address, subscription plan selection, and transaction history; and
- **Profile and Settings Data:** Any additional Personal Data you choose to include in your profile, preferences, or user settings on the IncomeCompliant platform or any other Scireat Group service.

3.2 Information Collected Automatically

When you access or use our websites, applications, or the IncomeCompliant platform, we and our authorized service providers automatically collect certain technical and usage data, including:

- **Log and Network Data:** IP address, browser type and version, operating system, referring URLs, pages viewed, time and date of access, session duration, error logs, and other standard web server log data;
- **Device Identifiers:** Device type, unique device identifiers, mobile network information, and hardware model where a mobile application is used;
- **Cookies and Similar Technologies:** As described in detail in Section 8 of this Privacy Policy, we use cookies, pixel tags, web beacons, local storage

objects, and similar tracking technologies to collect information about user behavior, session state, and platform performance; and

- **Usage and Analytics Data:** Feature usage patterns, click-stream data, workflow completion rates, error frequencies, and other analytics data collected by first-party and third-party analytics tools, used to improve the performance and usability of the IncomeCompliant platform and our other services.

3.3 Information from Third Parties

The Scireat Group may receive Personal Data about individuals from third-party sources, subject to those parties' own privacy policies and applicable law, including:

- **Data Brokers and Enrichment Providers:** Third-party data providers from whom we may obtain business contact data, firmographic data, or data enrichment information for enterprise sales and marketing purposes, subject to those providers' representations that they have lawful authority to share such data;
- **Integration Partners:** Payroll processors, accounting software vendors, human resources information systems (HRIS) vendors, and enterprise resource planning (ERP) platforms with which the IncomeCompliant platform integrates, pursuant to user-authorized data sharing;
- **Financial Institutions via Open Banking APIs:** Where a user or enterprise customer authorizes a connection between the IncomeCompliant platform and a financial institution, we may receive account-level financial data, transaction history, account balance information, and income verification data through open banking APIs, consistent with the authorization granted and applicable financial data sharing regulations; and
- **Payroll Processors:** Employer-authorized payroll data, including gross wages, net pay, deduction schedules, pay frequency, and tax withholding information, transmitted to the IncomeCompliant platform for income tracking and compliance purposes.

3.4 Health-Financial Intersection Data

In the course of providing compliance and income-tracking services through the IncomeCompliant platform and through Accelavest Financial Services LLC, the Scireat Group may receive, process, or generate data that constitutes Health-Financial Data as defined in Section 2. This category includes, without limitation:

- Insurance enrollment records that link an individual's health plan participation to payroll deductions, employer contributions, or taxable benefit values;
- Health Savings Account (HSA) and Flexible Spending Account (FSA) contribution, distribution, and balance data;
- Health-plan-linked income determinations, including data used to establish premium subsidy eligibility under the Affordable Care Act, Medicaid income thresholds, or CHIP eligibility; and
- Any other data that, in combination, identifies both an individual's health condition, health plan membership, or health care utilization and that individual's financial, income, or employment status.

Health-Financial Data is subject to the heightened protections described in Section 5 of this Privacy Policy. The Scireat Group does not collect Health-Financial Data beyond what is necessary for the services requested by the enterprise customer or individual user.

3.5 IncomeCompliant-Specific Data

Users of the IncomeCompliant platform may, in the course of using the platform's compliance, reporting, and income-tracking features, provide or generate the following categories of data:

- Income records, including gross income, net income, income sources, income verification documentation, and historical income data;
- Tax documents, including W-2 forms, 1099 forms, tax returns, and associated schedules, uploaded to or generated by the platform;

- Compliance submissions, including regulatory filings, income attestations, eligibility certifications, and supporting documentation prepared or transmitted through the platform;
- Employer-linked financial records, including employer identification numbers, payroll schedules, benefit deduction records, and employment verification data; and
- Government benefit eligibility data, including data related to Medicaid, SNAP, housing assistance, childcare subsidies, and other income-tested public benefit programs, to the extent such data is provided by or on behalf of the user for compliance tracking purposes.

3.6 Accelavest Financial Services Data

Accelavest Financial Services LLC, as an investment advisory and financial services subsidiary, collects additional categories of Personal Data from its clients in connection with the provision of investment advisory, financial planning, and related financial services, including:

- Investment account data, including brokerage account numbers, custodian information, account balances, portfolio holdings, transaction history, and investment objectives;
- Advisory relationship data, including investment advisory agreements, suitability assessments, risk tolerance questionnaires, and client profile information as required by applicable securities laws;
- Financial planning records, including retirement planning projections, estate planning summaries, tax planning analyses, cash flow projections, and goal-tracking data; and
- Regulatory and compliance records required under applicable federal and state securities laws and the Gramm-Leach-Bliley Act, including know-your-customer (KYC) documentation, anti-money laundering (AML) records, and customer identification program (CIP) records.

Data collected by Accelavest Financial Services LLC is subject to the GLBA financial privacy provisions described in Section 4.7 and Section 6.3 of this Privacy Policy, as well as applicable securities law requirements.

3.7 Sensitive Personal Information

Certain Personal Data we collect qualifies as Sensitive Personal Information under applicable law and is subject to heightened collection, use, and disclosure restrictions. The Scireat Group collects the following categories of Sensitive Personal Information only to the extent strictly necessary for the specified purposes:

- **Social Security Numbers and Government-Issued Identifiers:** Collected by the IncomeCompliant platform and Accelavest Financial Services LLC for identity verification, tax reporting compliance, and regulatory KYC obligations;
 - **Financial Account Numbers:** Collected via open banking integrations and direct user input for payment processing, income verification, and advisory account management, subject to encryption and access controls;
 - **Health Plan Identifiers:** Collected as part of Health-Financial Data for benefits administration and compliance purposes, subject to the heightened protections of Section 5;
 - **Biometric Data:** If and when the Scireat Group implements biometric authentication features (e.g., fingerprint or facial recognition for platform access), such data will be collected only with explicit, informed consent, and will not be sold, traded, or used for commercial purposes beyond authentication; and
 - **Precise Geolocation Data:** Collected only with explicit user consent, where a location-dependent feature of a Scireat Group service requires precise geolocation. Approximate geolocation (city or region level) may be inferred from IP address for fraud prevention and service localization purposes.
-

4. PURPOSES AND LEGAL BASES FOR PROCESSING

4.1 Service Delivery and Contract Performance

The Scireat Group processes Personal Data to deliver the services, products, and platform features that Users and enterprise customers have contracted for or requested. This includes creating and managing user accounts, processing subscription payments, providing access to the IncomeCompliant platform, generating compliance reports, facilitating open banking integrations, maintaining platform functionality, and responding to support requests. Processing for this purpose is necessary for the performance of a contract to which the User or enterprise customer is a party or for the taking of pre-contractual steps at the request of the data subject.

4.2 Regulatory Compliance and Legal Obligation

The Scireat Group processes Personal Data to comply with applicable federal and state laws, regulations, and regulatory orders, including but not limited to: the Gramm-Leach-Bliley Act (GLBA) and its implementing regulations; the Internal Revenue Code and IRS regulations governing tax reporting and record retention; the Securities Exchange Act and applicable SEC rules governing Accelavest Financial Services LLC; HIPAA and HITECH Act requirements applicable in Business Associate contexts; and applicable Kansas state law. Processing for this purpose is necessary for compliance with a legal obligation to which the Scireat Group is subject.

4.3 Fraud Prevention and Security (Legitimate Interests)

We process certain Personal Data, including IP addresses, device identifiers, log data, and behavioral analytics, to detect, prevent, and investigate fraud, unauthorized access, security incidents, and other harmful or unlawful activities. This processing is in the legitimate interests of the Scireat Group and our Users in maintaining the security and integrity of our platforms and data. Users may object to processing for this purpose under the conditions described in Section 12.4; however, where such processing is strictly necessary for the security of our services, the objection may not be honored with respect to those specific processing activities.

4.4 Product Improvement and Analytics (Legitimate Interests with Opt-Out)

We process usage data and analytics data to understand how our platforms are used, to identify usability issues and areas for improvement, to develop new features, and to optimize platform performance. This processing is carried out in our legitimate interests in improving our services and is conducted using pseudonymized or aggregated data wherever feasible. Users who object to this processing may opt out via the Privacy Preference Center available at scireat.com/privacy-requests or by contacting privacy@scireat.com. Opt-out will not affect core service functionality.

4.5 Marketing Communications (Consent-Based)

We send marketing and promotional communications by email only to individuals who have provided explicit, affirmative consent to receive such communications, or, in the case of existing customers, in compliance with applicable "soft opt-in" rules where permitted by law. Each marketing communication includes a clear, one-click unsubscribe mechanism. Withdrawing consent for marketing communications does not affect the lawfulness of processing carried out before withdrawal. We do not send marketing communications to individuals based on Health-Financial Data, PHI, or Sensitive Personal Information.

4.6 GDPR Article 6 Legal Bases

For individuals located in the European Economic Area or the United Kingdom, the following table maps each processing purpose to the applicable lawful basis under Article 6 of the GDPR (and, where applicable, Article 9 for special category data):

Processing Purpose	Lawful Basis (GDPR Article 6)	Additional Basis for Special Category Data (Article 9)
Account creation and management	Art. 6(1)(b) — Contract performance	N/A (general personal data)
Delivering IncomeCompliant platform services	Art. 6(1)(b) — Contract performance	Art. 9(2)(b) — Employment/social protection obligations (where applicable)
Payment processing and billing	Art. 6(1)(b) — Contract performance	N/A

Processing Purpose	Lawful Basis (GDPR Article 6)	Additional Basis for Special Category Data (Article 9)
Legal and regulatory compliance	Art. 6(1)(c) — Legal obligation	Art. 9(2)(g) — Substantial public interest (tax, AML, securities law)
Fraud prevention and security monitoring	Art. 6(1)(f) — Legitimate interests	N/A
Product analytics and improvement	Art. 6(1)(f) — Legitimate interests	N/A (pseudonymized data used wherever possible)
Marketing communications	Art. 6(1)(a) — Consent	N/A
Health-Financial Data processing	Art. 6(1)(b) — Contract; Art. 6(1)(c) — Legal obligation	Art. 9(2)(b) — Employment/social protection; Art. 9(2)(h) — Health or social care management
International data transfers (EEA)	Art. 6(1)(b) or (c) as applicable	Art. 46 SCCs / Art. 45 Adequacy Decision as transfer mechanism
Responding to legal process and law enforcement	Art. 6(1)(c) — Legal obligation; Art. 6(1)(f) — Legitimate interests	Art. 9(2)(g) — Substantial public interest as applicable

4.7 GLBA Financial Data Processing

Accelavest Financial Services LLC is a financial institution subject to the privacy and safeguards provisions of the Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801–6809) and the implementing regulations of the Federal Trade Commission (16 C.F.R. Part 314, as amended by the FTC Safeguards Rule, 2023 revisions). In compliance with GLBA:

- Accelavest Financial Services LLC provides its customers with an initial GLBA Privacy Notice at the time of establishing a customer relationship and annually thereafter;
- Customers of Accelavest Financial Services LLC have the right to opt out of certain disclosures of their nonpublic personal information (NPI) to non-affiliated third parties, subject to the exceptions permitted by GLBA (e.g., disclosures necessary to effect, administer, or enforce a transaction, or as required by law);

- Accelavest Financial Services LLC maintains a comprehensive written information security program (WISP) pursuant to the FTC Safeguards Rule, including designation of a qualified individual responsible for overseeing the WISP, periodic risk assessments, and implementation of technical, administrative, and physical safeguards appropriate to the size and complexity of the business and the sensitivity of customer financial information; and
 - Opt-out requests from Accelavest Financial Services LLC customers may be directed to financial-privacy@scireat.com.
-

5. HIPAA-ADJACENT PROTECTIONS FOR HEALTH-FINANCIAL DATA

5.1 Scope of Health-Financial Data Practices

The Scireat Group recognizes that a number of its core service offerings, particularly the IncomeCompliant platform and Accelavest Financial Services LLC's benefit planning capabilities, involve the intersection of health data and financial data in ways that implicate significant privacy interests. While members of the Scireat Group may not qualify as HIPAA Covered Entities in all operational contexts, and while the full technical scope of HIPAA may not attach to every transaction, we voluntarily adopt HIPAA-equivalent privacy and security standards — collectively, our "**Health-Financial Data Standards**" — for all Health-Financial Data as defined in Section 2. This commitment reflects our belief that individuals whose health and financial information intersects in our systems deserve the highest degree of protection available under federal health privacy law, regardless of whether such protection is legally mandated in a given context.

5.2 Minimum Necessary Standard

Consistent with the HIPAA Minimum Necessary standard (45 C.F.R. § 164.502(b)), the Scireat Group limits access to, use of, and disclosure of Health-Financial Data to the minimum amount of information necessary to accomplish the stated, authorized purpose. We do not access, use, or disclose more Health-Financial Data than is

reasonably necessary to provide the specific service or function requested by the enterprise customer or individual user. All Scireat Group workforce members with access to Health-Financial Data are trained on the Minimum Necessary standard and are subject to role-based access controls that restrict their access to only the Health-Financial Data required to perform their job functions.

5.3 Permitted Uses and Disclosures of Health-Financial Data

The Scireat Group permits use and disclosure of Health-Financial Data only for the following purposes:

- **Payment Facilitation:** Processing premium payments, HSA and FSA contributions and distributions, and other financial transactions directly linked to health plan administration;
- **Benefits Administration:** Performing income and eligibility determinations for employer-sponsored health benefit programs, ACA premium tax credit calculations, Medicaid and CHIP eligibility assessments, and similar benefits administration functions on behalf of enterprise customers;
- **Legal and Regulatory Compliance:** Responding to lawful court orders, regulatory agency requests, IRS reporting obligations, and other legally mandated disclosures as described in Section 6.5; and
- **De-Identified Analytics:** Generating aggregated, de-identified statistical analyses for product improvement, benchmarking, and research purposes, provided that the data has been de-identified in accordance with Section 5.5 of this Privacy Policy.

The following uses and disclosures of Health-Financial Data are expressly **prohibited**:

- Use of Health-Financial Data for marketing, advertising, or promotional purposes of any kind, whether by the Scireat Group or any third party;
- Sale, rental, exchange, or other disclosure of Health-Financial Data to third parties for commercial consideration or any purpose not authorized by this Section 5.3 or the applicable BAA; and

- Use of Health-Financial Data beyond the Minimum Necessary standard, or for any purpose not disclosed to the individual at the time of collection.

5.4 Business Associate Agreement Policy

When the IncomeCompliant platform or any other Scireat Group service integrates with or processes data from a HIPAA Covered Entity — including employer-sponsored health plans, group health insurance carriers, third-party plan administrators, or other Covered Entities as defined in 45 C.F.R. § 160.103 — the Scireat Group requires the execution of a Business Associate Agreement (BAA) pursuant to 45 C.F.R. § 164.504(e) before any Protected Health Information flows between the Covered Entity and the Scireat Group system. No PHI is ingested, processed, or stored by the Scireat Group in connection with a Covered Entity relationship unless a fully executed BAA is in place. The Scireat Group's standard BAA template is available to prospective Covered Entity partners upon request to privacy@scireat.com. Enterprise customers seeking to configure IncomeCompliant integrations that will involve PHI flows from a Covered Entity must notify their Scireat account manager before activating such integrations, so that the appropriate BAA can be executed in advance.

5.5 De-Identification Standards

The Scireat Group de-identifies Health-Financial Data before using it for aggregated analytics, product benchmarking, or any other secondary purpose not involving the provision of services to the specific enterprise customer or individual from whom the data originated. De-identification is performed using one of the following methods:

- **Safe Harbor Method (45 C.F.R. § 164.514(b)(2)):** Removal of all 18 categories of HIPAA identifiers specified in the Safe Harbor method, including name, geographic data smaller than state level, dates (other than year) for individuals over 89, telephone numbers, fax numbers, email addresses, Social Security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate or license numbers, vehicle identifiers, device identifiers, web URLs, IP addresses, biometric identifiers, full-face photographs, and any other unique identifying number

or code, along with verification that the remaining information does not identify any individual and there is no reasonable basis to believe it could; or

- **Expert Determination Method (45 C.F.R. § 164.514(b)(1)):**

Engagement of a qualified statistical expert who applies generally accepted statistical and scientific principles to determine and document that the risk of identifying an individual from the de-identified dataset is very small.

Re-identification of de-identified data is strictly prohibited unless required by law or authorized by the enterprise customer and individual for a specific, documented purpose.

5.6 Individual Rights Regarding Health-Financial Data

Individuals whose Health-Financial Data is processed by the Scireat Group have the following rights with respect to that data, exercisable by contacting privacy@scireat.com:

- **Right to Access:** The right to request a copy of the Health-Financial Data held by the Scireat Group pertaining to the individual, subject to verification of identity;
- **Right to Amend:** The right to request correction of inaccurate or incomplete Health-Financial Data, subject to the Scireat Group's verification of the inaccuracy and any applicable legal record-retention requirements;
- **Right to Restrict Processing:** The right to request restriction of the use of Health-Financial Data beyond the purposes described in Section 5.3, where such restriction is technically and operationally feasible given the services being provided; and
- **Right to an Accounting of Disclosures:** The right to request a record of disclosures of Health-Financial Data made by the Scireat Group to third parties for the six-year period preceding the request, including the date of disclosure, the identity of the recipient, and the purpose of the disclosure.

5.7 Health Data Security Safeguards

The Scireat Group implements the following technical and organizational security safeguards specifically for Health-Financial Data:

- **Encryption at Rest:** All Health-Financial Data is encrypted at rest using AES-256 encryption;
- **Encryption in Transit:** All Health-Financial Data transmitted over public or private networks is encrypted using Transport Layer Security (TLS) version 1.3 or higher;
- **Role-Based Access Controls (RBAC):** Access to Health-Financial Data is granted on a least-privilege, role-based basis; access rights are reviewed on a quarterly basis and revoked promptly upon change of role or employment termination;
- **Multi-Factor Authentication (MFA):** All workforce members and Authorized Users with access to systems containing Health-Financial Data are required to authenticate using multi-factor authentication;
- **Audit Logging:** All access to, modification of, and disclosure of Health-Financial Data is logged in tamper-evident audit logs, retained for a minimum of six years; and
- **Vulnerability Management:** Systems processing Health-Financial Data are subject to regular automated vulnerability scanning and annual third-party penetration testing, with critical findings remediated within 30 days of discovery.

5.8 FTC Health Breach Notification Rule

To the extent that the Scireat Group operates health applications or services involving personal health records that are not covered by HIPAA, the Scireat Group complies with the Federal Trade Commission's Health Breach Notification Rule (16 C.F.R. Part 318), as amended in 2024. In the event of a breach of security of individually identifiable health information covered by the FTC Health Breach Notification Rule, the Scireat Group will notify affected individuals within 60 calendar days of discovery of the breach, and will notify the FTC as required by the

Rule. Where the breach affects 500 or more residents of a state or jurisdiction, notice will also be provided to prominent media outlets in the affected area, consistent with Rule requirements.

5.9 State Consumer Health Data Laws

Multiple U.S. states have enacted or are in the process of enacting consumer health data privacy statutes that impose requirements beyond those of HIPAA with respect to health data processed by entities that do not qualify as HIPAA Covered Entities. The Scireat Group acknowledges and commits to compliance with these statutes, including:

- **Washington My Health My Data Act (MHMDA), S.B. 1155 (2023):**
With respect to Washington state consumers, the Scireat Group complies with the MHMDA's requirements concerning consumer health data, including: honoring consumers' rights to access, delete, and withdraw consent for collection of consumer health data; refraining from selling consumer health data without valid authorization; implementing a consumer health data privacy policy specific to Washington residents; and obtaining authorization before sharing consumer health data with third parties for purposes beyond those necessary for the requested services; and
- **Emerging State Statutes:** As additional states enact consumer health data privacy laws, the Scireat Group commits to monitor, assess, and achieve compliance with such statutes and to extend equivalent protections to users in affected states on a timely basis. Updates reflecting new state law compliance commitments will be published at scireat.com/privacy-policy/history.

6. HOW WE SHARE YOUR INFORMATION

6.1 Within the Scireat Group

Personal Data may be shared among Scireat LLC, Sciorbis Business Group LLC, Accelavest Financial Services LLC, and Mersellus LLC for internal business,

operational, and administrative purposes consistent with this Privacy Policy. All intra-group data sharing is governed by binding intra-group data sharing agreements that impose equivalent data protection obligations on each receiving entity. Intra-group data sharing does not result in any additional uses of Personal Data beyond those disclosed in this Privacy Policy, and does not constitute a "sale" or "sharing" of Personal Data under applicable law.

6.2 Service Providers and Processors

We engage third-party service providers to perform functions on our behalf that are necessary for the delivery and operation of our services. These service providers are authorized to access and process Personal Data only as necessary to perform the specific services contracted, are bound by written data processing agreements that impose GDPR Article 28-compliant obligations and equivalent protections under applicable U.S. law, and are prohibited from using Personal Data for their own independent purposes. Current categories of service providers and the categories of Personal Data disclosed to each include:

- **Cloud Hosting and Infrastructure Providers:** SOC 2 Type II-certified cloud infrastructure providers host our production systems, databases, and backups. Data disclosed: all categories of Personal Data processed by the IncomeCompliant platform and Scireat Group websites, subject to encryption;
- **Payment Processors:** PCI DSS Level 1-certified payment processors handle credit and debit card transactions. Data disclosed: payment card data (processed directly by the payment processor; Scireat does not receive or store full card numbers), billing address, and transaction amounts;
- **Analytics Vendors:** Web and product analytics providers receive pseudonymized or anonymized usage and behavioral data. Data disclosed: pseudonymized user identifiers, feature usage data, page view and click-stream data, session duration, and IP addresses (anonymized);
- **Customer Support Platforms:** Cloud-based customer support ticket and CRM systems receive support request data. Data disclosed: name, email

address, account information, and the content of support communications;
and

- **Email and Communication Service Providers:** Providers of transactional and marketing email delivery services. Data disclosed: email address, name, and communication preference data.

A current list of our primary service providers is available at scireat.com/subprocessors. We review and update our service provider relationships on an ongoing basis and will provide notice of material changes as described in Section 7.4.

6.3 Financial Institution Partners

For the purposes of enabling the IncomeCompliant platform's open banking integrations and Accelavest Financial Services LLC's investment advisory and custodian account management services, we may share Personal Data with financial institution partners, including banks, broker-dealers, custodians, and payment networks. All such sharing is subject to: user-authorized data sharing consent obtained at the time of integration activation; GLBA-compliant data sharing agreements; and limitations on the financial institution partner's use of Personal Data to the purposes for which sharing was authorized. Financial institution partners are not permitted to use Personal Data received from the Scireat Group for their own marketing, solicitation, or data monetization purposes.

6.4 Business Associates

As described in Section 5.4, when the Scireat Group processes Protected Health Information or Health-Financial Data in connection with the services of a HIPAA Covered Entity, we will disclose such data only to Business Associates with whom a fully executed BAA is in place. All Business Associate relationships are documented in our BAA registry, maintained by the Scireat LLC Privacy Officer.

6.5 Legal and Regulatory Disclosures

The Scireat Group may disclose Personal Data when we have a good-faith belief that disclosure is required or permitted by applicable law, including:

- In response to a valid court order, subpoena, search warrant, or other legal process issued by a court or governmental authority with proper jurisdiction;
- To comply with lawful requests from governmental regulatory agencies, including the Internal Revenue Service, the Securities and Exchange Commission, the Federal Trade Commission, Kansas state regulatory agencies, and other agencies with regulatory jurisdiction over Scireat Group activities;
- To enforce our Terms of Service or other applicable agreements, or to protect the legal rights, property, or safety of the Scireat Group, our Users, or third parties; and
- In connection with national security or law enforcement requirements as mandated by applicable law.

Where legally permitted to do so, the Scireat Group will provide advance notice to affected individuals before disclosing their Personal Data pursuant to legal process. We publish aggregate transparency report data regarding legal demands received at scireat.com/transparency annually.

6.6 Business Transfers

In the event of a merger, acquisition, reorganization, asset sale, or other corporate transaction involving all or a substantial portion of the Scireat Group's business or assets, Personal Data may be transferred to the successor entity as part of such transaction. The Scireat Group will provide affected individuals with not less than 30 calendar days' advance written notice of any such transfer by email to the address on file and by prominent notice on our website. The successor entity will be required to honor the privacy commitments set forth in this Privacy Policy with respect to all Personal Data received. In the event the successor entity intends to process Personal Data in a manner materially inconsistent with this Privacy Policy, affected individuals will be provided with an opportunity to delete their data before such changes take effect.

6.7 With Your Consent

We will share Personal Data with third parties for any purpose not described in Sections 6.1 through 6.6 only with the prior, express, and informed consent of the affected individual. Consent obtained for sharing purposes will be documented and will describe the specific third party recipient, the categories of Personal Data to be shared, and the purpose of sharing. Consent may be withdrawn at any time by contacting privacy@scireat.com, and withdrawal of consent will not affect the lawfulness of sharing carried out before the withdrawal.

6.8 Categories of Personal Information Disclosed to Service Providers in the Preceding 12 Months

The following table is provided in compliance with the CCPA/CPRA and identifies the categories of personal information the Scireat Group has disclosed to service providers and contractors for business purposes during the 12-month period preceding the Effective Date of this Privacy Policy:

Category of Personal Information (CCPA Categories)	Disclosed to Service Providers for Business Purposes?	Categories of Service Providers Receiving this Data	Sold or Shared for Cross-Context Behavioral Advertising?
Identifiers (name, email, IP address, account ID)	Yes	Cloud hosting, analytics, customer support, email delivery	No (not sold); Limited sharing for analytics subject to opt-out
Personal information under Cal. Civil Code § 1798.80 (financial account numbers, SSNs)	Yes	Cloud hosting (encrypted), payment processors, financial institutions	No
Commercial information (transaction history, subscription data)	Yes	Payment processors, cloud hosting, customer support	No
Internet or other electronic network activity information (usage	Yes	Analytics vendors, cloud hosting, security monitoring	No (not sold); Limited sharing for analytics subject to opt-out

Category of Personal Information (CCPA Categories)	Disclosed to Service Providers for Business Purposes?	Categories of Service Providers Receiving this Data	Sold or Shared for Cross-Context Behavioral Advertising?
data, log data)		services	
Geolocation data (approximate, IP-derived)	Yes	Analytics vendors, fraud prevention services	No
Professional or employment-related information	Yes	Cloud hosting, IncomeCompliant platform subprocessors	No
Financial data (income records, tax documents, account data)	Yes	Cloud hosting (encrypted), financial institution partners, regulatory subprocessors	No
Sensitive Personal Information (SSN, financial account numbers, health plan identifiers)	Yes (limited; encrypted)	Cloud hosting (encrypted), payment processors, regulatory compliance processors	No
Inferences drawn from personal information (user preferences, usage patterns)	Yes	Analytics vendors (pseudonymized)	No

The Scireat Group does not sell Personal Information. To the extent that the sharing of pseudonymized usage data or advertising-related data with analytics or advertising vendors constitutes "sharing" for cross-context behavioral advertising under CCPA/CPRA, California residents may opt out of such sharing as described in Section 12.3.

7. SAAS-SPECIFIC PROVISIONS — INCOMECOMPLIANT

7.1 Platform Architecture and Data Isolation

The IncomeCompliant platform is built on a multi-tenant SaaS architecture. Each enterprise customer's data is logically isolated from the data of all other enterprise customers through the use of separate data partitions, tenant-specific encryption keys, and access control policies enforced at the application and infrastructure layers. No enterprise customer's Authorized Users can access, view, or query the data of any other enterprise customer. Cross-tenant data analysis is not performed except on fully de-identified, aggregated datasets as described in Section 5.5. Scireat LLC conducts periodic technical audits of tenant data isolation controls to verify their effectiveness.

7.2 Customer Data vs. Scireat Operational Data

For purposes of the IncomeCompliant platform, the Scireat Group distinguishes between two categories of data:

- **Customer Data:** Data that enterprise customers and their Authorized Users upload to, enter into, generate through, or transmit via the IncomeCompliant platform in connection with their use of the service, including income records, tax documents, employee financial data, and compliance submissions. Customer Data is controlled by the enterprise customer, and Scireat LLC processes Customer Data solely as a Data Processor acting on the documented instructions of the enterprise customer. Scireat LLC does not access Customer Data except as necessary to deliver the contracted services, to fulfill legal obligations, or to respond to documented support requests from the enterprise customer; and
- **Operational Data:** Data that Scireat LLC collects about how the enterprise customer and its Authorized Users interact with the IncomeCompliant platform, including log data, feature usage metrics, session data, and support interaction records. Operational Data is controlled by Scireat LLC and is used for service delivery, security monitoring, product improvement, and business operations as described in this Privacy Policy.

7.3 Data Processing Agreements

Enterprise customers of the IncomeCompliant platform who are subject to the GDPR, UK GDPR, or other data protection frameworks that require formal data processing agreements may execute a Data Processing Agreement (DPA) with Scireat LLC. The DPA governs Scireat LLC's role as a Data Processor with respect to Customer Data under GDPR Article 28, and includes the technical and organizational measures implemented by Scireat LLC, subprocessor authorization and notification procedures, data subject rights assistance obligations, breach notification timelines, and data return and deletion provisions. Scireat LLC's standard DPA is available upon request to privacy@scireat.com. Enterprise customers may also execute custom DPAs that supplement the standard terms, subject to Scireat LLC's approval.

7.4 Subprocessors

Scireat LLC engages certain sub-processors to assist in providing the IncomeCompliant platform services, including cloud infrastructure providers, database services, encryption key management services, and monitoring tools. A current list of all IncomeCompliant subprocessors, including name, location, and function, is maintained and publicly available at scireat.com/subprocessors. Enterprise customers who have executed a DPA will receive not less than 30 calendar days' advance written notice of any intended addition to or replacement of a material subprocessor, during which period the enterprise customer may object to the change in writing. If a reasonable objection is raised and the parties cannot resolve the matter, the enterprise customer may terminate the applicable subscription as provided in the IncomeCompliant Service Agreement.

7.5 Data Portability and Export

Enterprise customers have the right to export their Customer Data from the IncomeCompliant platform at any time during their active subscription term and for a period of 90 calendar days following the termination or expiration of the subscription (the "Post-Termination Export Period"). Customer Data may be exported in the following machine-readable formats, as available within the platform: Comma-Separated Values (CSV), JavaScript Object Notation (JSON), and Portable Document Format (PDF). Export functionality is accessible through the

platform's administrative interface. After the Post-Termination Export Period has expired, Customer Data will be subject to deletion in accordance with Section 7.6.

7.6 Post-Termination Data Deletion

Following the termination or expiration of an enterprise customer's IncomeCompliant subscription:

- **Production Systems:** Customer Data will be deleted from all production databases and application servers within 90 calendar days of the account termination date;
- **Backup Systems:** Customer Data contained in backup snapshots and archival storage will be deleted or overwritten within 180 calendar days of the account termination date, consistent with our backup rotation schedule;
- **Certified Deletion:** Enterprise customers may request written certification of the deletion of their Customer Data by submitting a certified deletion request to privacy@scireat.com. Certified deletion requests will be fulfilled within 30 calendar days of receipt, and a written confirmation of deletion will be provided; and
- **Retained Data:** Notwithstanding the foregoing, Scireat LLC may retain certain Operational Data and anonymized or aggregated data derived from Customer Data for legitimate legal, regulatory, and business purposes, provided that such retained data does not permit identification of the individual data subjects of the terminated enterprise customer.

7.7 Uptime, Security, and Compliance SLAs

The IncomeCompliant platform is committed to high availability and security performance. Specific uptime commitments, scheduled maintenance windows, and SLA credit terms are set forth in the IncomeCompliant Service Agreement applicable to each enterprise customer's subscription. SOC 2 Type II audit reports for the IncomeCompliant platform are available to enterprise customers under a mutual non-disclosure agreement upon request to privacy@scireat.com. Scireat LLC conducts annual third-party SOC 2 audits covering the Security, Availability, and Confidentiality Trust Service Criteria applicable to the IncomeCompliant platform.

7.8 Automated Decision-Making in IncomeCompliant

The IncomeCompliant platform uses automated logic and algorithmic processing to assist enterprise customers and their Authorized Users in performing income eligibility determinations, compliance flag assessments, and regulatory threshold calculations. Users should be aware of the following with respect to automated decision-making in the platform:

- **Nature of Automation:** The platform applies predefined rules, income thresholds, and regulatory parameters specified by applicable law or by the enterprise customer's configuration to determine compliance status, flag potential income reporting discrepancies, and assess eligibility for benefit programs. These determinations are rule-based and transparent, not opaque machine-learning models that operate without human oversight;
 - **Human Review — CCPA/CPRA:** California residents have the right to request human review of any automated decision made by the IncomeCompliant platform that significantly affects them, pursuant to CCPA/CPRA Section 1798.185(a)(16) and the 2026 CPPA Automated Decision-Making Technology regulations effective January 1, 2027. Requests for human review may be submitted to privacy@scireat.com;
 - **Human Review — GDPR Article 22:** EEA and UK residents have the right not to be subject to a decision based solely on automated processing, including profiling, that produces legal or similarly significant effects concerning them, except as permitted by GDPR Article 22(2). Where automated decisions on the IncomeCompliant platform produce legally significant effects for EEA or UK data subjects, the enterprise customer and Scireat LLC will ensure that a human review mechanism is available; and
 - **Opt-Out:** To the extent technically and operationally feasible, enterprise customers may configure the IncomeCompliant platform to require human authorization of all compliance determinations and eligibility assessments, thereby limiting reliance on fully automated decisions.
-

8. COOKIES AND TRACKING TECHNOLOGIES

8.1 Types of Cookies Used

The Scireat Group uses the following categories of cookies and similar tracking technologies on our websites and within the IncomeCompliant platform:

- **Strictly Necessary Cookies:** These cookies are essential for the operation of our websites and the IncomeCompliant platform. They enable core functionality such as session management, authentication, security token validation, and CSRF protection. These cookies cannot be disabled without impairing the basic functionality of the service. No consent is required for strictly necessary cookies;
- **Functional Cookies:** These cookies enable enhanced functionality and personalization, including remembering user preferences, language settings, and interface customizations. Disabling these cookies may affect user experience but will not impair core service functionality;
- **Analytics Cookies:** These cookies collect aggregated and pseudonymized data about how users interact with our websites and platform, including pages visited, time spent, features used, and error events. This data is used to improve platform usability and performance. Analytics cookies are subject to user consent for EEA and UK users; and
- **Marketing Cookies:** These cookies track users across websites and are used to deliver targeted advertising and measure advertising campaign effectiveness. Marketing cookies are used only with explicit consent and are not deployed within the authenticated IncomeCompliant platform interface.

8.2 Third-Party Tracking

We deploy Google Analytics with IP anonymization enabled on our public-facing websites to analyze website traffic and user behavior patterns. IP anonymization ensures that IP addresses are truncated before storage. We may also deploy advertising pixels (such as LinkedIn Insight Tag and similar tools) on our marketing pages to measure campaign effectiveness and to enable targeted advertising on third-party platforms, subject to user consent. Third-party tracking technologies are

governed by the privacy policies of the respective third-party providers, and we encourage users to review those policies. Users may opt out of Google Analytics data collection across all websites by installing the Google Analytics Opt-out Browser Add-on.

8.3 Cookie Consent and Management

Upon first visiting any Scireat Group public-facing website, users located in the EEA, UK, and other jurisdictions requiring prior consent for non-essential cookies are presented with a cookie consent banner that allows them to accept all cookies, reject non-essential cookies, or configure their preferences by category. Users may change their cookie preferences at any time by accessing the Privacy Preference Center available at scireat.com/cookie-preferences or via the cookie preference link in the footer of our websites. Withdrawal of consent for non-essential cookies will not affect the functionality of strictly necessary cookies.

8.4 Do Not Track and Global Privacy Control Signals

The Scireat Group honors the Global Privacy Control (GPC) browser signal as a valid opt-out of the sale and sharing of Personal Information for California residents under CCPA/CPRA Section 1798.135(e). When a GPC signal is detected from a California resident's browser session, we will treat the signal as a request to opt out of sharing for cross-context behavioral advertising and will suppress the deployment of marketing and advertising tracking technologies for that session. With respect to the Do Not Track (DNT) browser signal, there is currently no uniform industry standard for honoring DNT signals; however, we encourage users who wish to opt out of analytics tracking to use the mechanisms described in Sections 8.3 and 12.3.

9. DATA RETENTION

9.1 General Retention Principles

The Scireat Group retains Personal Data only for as long as necessary to fulfill the purposes for which it was collected, as required by applicable law or regulation, or as necessary to resolve disputes, enforce agreements, and maintain business records. We do not retain Personal Data in identifiable form for longer than is required by

these criteria, and we periodically review our data holdings to identify and securely delete data that has exceeded its retention period.

9.2 Retention Schedule

The following table sets forth our standard retention periods for the primary categories of Personal Data we process:

Data Category	Retention Period	Legal or Business Basis for Retention Period
Account and Profile Data	Duration of the customer or user relationship, plus 7 years following account closure	Contract performance; IRS record-keeping requirements; applicable statute of limitations
Financial Records (income records, tax documents, transaction history)	7 years from the date of the record	IRS requirements (26 C.F.R. § 1.6001-1); GLBA record retention; applicable state financial regulations
Health-Financial Data (HSA/FSA data, health-plan-linked income data, PHI in BAA contexts)	6 years from the date of creation or last effective date, whichever is later	HIPAA-equivalent standard (45 C.F.R. § 164.530(j)); BAA retention obligations
Accelavest Financial Services Client Records	5 years from the date of the record for most records; as required by SEC and FINRA regulations for specific record categories	SEC Regulation S-P; GLBA; applicable securities law record retention rules
Marketing and Communication Preference Data	3 years from the date of last interaction, or until opt-out is received, whichever is earlier	CAN-SPAM Act; GDPR consent record obligations; CCPA/CPRA
Log and Technical Data (server logs, access logs, security logs)	13 months from the date of generation	Security monitoring best practices; fraud investigation requirements; GDPR data minimization
Backup Data	Deleted within 180 calendar days following a deletion request or account termination	Backup rotation schedule; GDPR and CCPA/CPRA deletion rights
Cookie and Analytics	13 months for analytics	GDPR data minimization;

Data Category	Retention Period	Legal or Business Basis for Retention Period
Data	session data; cookie preferences retained for 12 months	CNIL and ICO guidance on analytics cookie retention
Support and Correspondence Records	3 years from date of last interaction	Dispute resolution; legal claim defense; service improvement
Business Associate Agreement records and PHI disclosure accounting	6 years from the date of creation or last effective date	45 C.F.R. § 164.530(j); BAA obligations

9.3 Criteria for Determining Retention Periods

Where a retention period is not specified in Section 9.2 or in an applicable legal or contractual requirement, we determine appropriate retention periods by reference to the following criteria: the nature and sensitivity of the Personal Data; the purposes for which the Personal Data was collected and whether those purposes have been fulfilled; the potential risk of harm from unauthorized use or disclosure; the applicable statutory limitation periods for legal claims; and our legal obligations under applicable law. Retention periods are reviewed and updated at least annually by the Scireat LLC Privacy Officer.

9.4 Secure Deletion Procedures

Upon the expiration of the applicable retention period, Personal Data is deleted or de-identified using industry-standard secure deletion procedures appropriate to the medium on which the data is stored, including cryptographic erasure for encrypted data, secure overwriting for disk-based storage, and physical destruction for any hardware on which Personal Data is stored in non-erasable form. Deletion procedures are documented in our Data Lifecycle Management Policy, available to enterprise customers upon request under NDA.

10. DATA SECURITY

10.1 Technical Safeguards

The Scireat Group implements comprehensive technical security measures to protect Personal Data from unauthorized access, disclosure, alteration, and destruction, including:

- **Encryption at Rest:** All Personal Data stored in Scireat Group production databases and data stores is encrypted using AES-256 encryption. Encryption keys are managed through a dedicated key management service with strict access controls and annual key rotation;
- **Encryption in Transit:** All data transmitted between clients and Scireat Group servers, and between Scireat Group services, is encrypted using Transport Layer Security (TLS) version 1.3 or higher. TLS 1.0 and 1.1 are disabled across all Scireat Group infrastructure;
- **Multi-Factor Authentication:** MFA is required for all workforce member access to production systems, administrative consoles, and systems containing Personal Data. MFA is available to and encouraged for all Authorized Users of the IncomeCompliant platform;
- **Role-Based Access Control:** Access to Personal Data is governed by least-privilege RBAC policies, with access rights provisioned based on documented job functions and reviewed quarterly;
- **Vulnerability Scanning:** Automated vulnerability scanning is performed on all internet-facing and internal systems on a continuous or weekly basis, with critical and high severity findings escalated to the security team for immediate remediation; and
- **Penetration Testing:** Annual third-party penetration tests are conducted by qualified security firms against the IncomeCompliant platform and critical Scireat Group infrastructure. Critical findings are remediated within 30 days and high-severity findings within 60 days of discovery.

10.2 Administrative Safeguards

The Scireat Group maintains the following administrative security controls:

- **Information Security Policies:** A comprehensive suite of written information security policies, including an Acceptable Use Policy, Access Control Policy, Incident Response Plan, and Data Classification Policy, govern all Scireat Group information security practices;
- **Workforce Training:** All Scireat Group workforce members complete mandatory security awareness training at hire and annually thereafter, covering phishing awareness, data handling procedures, and incident reporting obligations;
- **Vendor Risk Management:** Third-party service providers and subprocessors are subject to security due diligence assessment before engagement, and periodic security reviews during the relationship, to ensure they maintain security standards commensurate with the sensitivity of the Personal Data they process; and
- **Designated Security Officer:** Scireat LLC has designated a qualified individual as Security Officer responsible for overseeing and implementing the Scireat Group's information security program, consistent with the requirements of the FTC Safeguards Rule and HIPAA Security Rule equivalent standards.

10.3 Physical Safeguards

The Scireat Group's production infrastructure is hosted in data centers operated by SOC 2 Type II-certified cloud service providers. These facilities implement physical access controls including, at minimum: biometric and key card access controls at data center entrances; 24/7 on-site security personnel; video surveillance of all access points and server rooms; environmental controls for temperature, humidity, and fire suppression; and physical separation of customer-facing infrastructure from internal systems. No Customer Data or Personal Data is stored on local workstations or portable media without encryption and prior authorization.

10.4 Incident Response and Breach Notification Timeline

The Scireat Group maintains a written Incident Response Plan that governs our response to suspected or confirmed Data Breaches. In the event of a confirmed Data Breach involving Personal Data, we will:

- Contain the breach and preserve evidence within 24 hours of discovery;
- Conduct a preliminary assessment of the scope and severity of the breach within 72 hours of discovery;
- Notify affected EEA and UK supervisory authorities within 72 hours of becoming aware of a reportable breach, where required by GDPR Article 33;
- Notify affected EEA and UK data subjects without undue delay if the breach is likely to result in a high risk to their rights and freedoms, as required by GDPR Article 34;
- Notify affected U.S. state residents in accordance with applicable state breach notification laws, including the Kansas Protection of Consumer Information Act (K.S.A. 50-7a01 et seq.), within the timeframes required by each state's law;
- Notify affected individuals whose Health-Financial Data is involved in compliance with the FTC Health Breach Notification Rule within 60 calendar days of discovery; and
- Notify enterprise customers of breaches affecting their Customer Data within the timeframes specified in the applicable DPA or Service Agreement, and in no event later than 72 hours after confirmation of the breach.

11. INTERNATIONAL DATA TRANSFERS

11.1 Transfers from the European Economic Area

Where the Scireat Group transfers Personal Data of individuals located in the European Economic Area to the United States or to other countries that the European Commission has not determined to provide an adequate level of data

protection, we rely on the following transfer mechanisms to ensure that such transfers comply with Chapter V of the GDPR:

- **Standard Contractual Clauses (SCCs):** We incorporate the Standard Contractual Clauses adopted by the European Commission under Implementing Decision (EU) 2021/914 of June 4, 2021 (the "2021 SCCs") into our agreements with EEA-based enterprise customers and their Authorized Users. For controller-to-processor transfers, we use the Module 2 SCCs; for processor-to-subprocessor transfers, we use the Module 3 SCCs. A copy of our executed SCCs is available upon request to privacy@scireat.com;
- **EU-US Data Privacy Framework:** Where Scireat LLC has self-certified under the EU-US Data Privacy Framework (DPF), as administered by the U.S. Department of Commerce, we may rely on the DPF as a transfer mechanism for transfers covered by our certification. Our DPF participation status is publicly verifiable at the DPF list maintained by the Department of Commerce; and
- **Transfer Impact Assessments:** We conduct and document Transfer Impact Assessments (TIAs) in connection with EEA data transfers to assess the legal landscape of the destination country and, where necessary, implement supplementary technical and organizational measures to ensure an essentially equivalent level of protection.

11.2 Transfers from the United Kingdom

For transfers of Personal Data of individuals in the United Kingdom to countries not covered by a UK adequacy regulation, we rely on the UK International Data Transfer Agreement (UK IDTA) issued by the UK Information Commissioner's Office, or the UK Addendum to the 2021 EU SCCs, as applicable. Our UK IDTA or UK Addendum is incorporated into agreements with UK-based enterprise customers and is available upon request to privacy@scireat.com.

11.3 Other International Transfers

For transfers of Personal Data originating from other jurisdictions with international data transfer requirements, including Canada (PIPEDA), Switzerland (Swiss Federal Act on Data Protection), and other countries with applicable transfer restrictions, we apply transfer mechanisms recognized under the applicable local law, including adequacy determinations where available, SCCs or equivalent contractual clauses, and binding corporate rules or equivalent intra-group transfer mechanisms where appropriate. We monitor developments in international data transfer law and update our transfer mechanisms accordingly.

11.4 How to Obtain Transfer Mechanism Documentation

Individuals and enterprise customers may request a copy of the applicable data transfer mechanisms in place for transfers of their Personal Data by contacting privacy@scireat.com. We will provide the requested documentation within 15 business days, subject to any confidentiality redactions required to protect the legitimate business interests of other parties.

12. YOUR RIGHTS AND CHOICES

Individuals whose Personal Data is processed by the Scireat Group have rights with respect to their data under applicable federal and state law. The specific rights available depend on the individual's jurisdiction and the nature of the Personal Data being processed. The Scireat Group is committed to honoring all applicable data subject rights promptly and without discrimination.

12.1 Rights Under U.S. Federal Law

- **GLBA Financial Privacy Rights:** Customers of Accelavest Financial Services LLC have the right to receive an annual privacy notice describing the categories of nonpublic personal information collected and the circumstances under which such information may be shared with affiliated and non-affiliated third parties. Customers have the right to opt out of certain disclosures of their NPI to non-affiliated third parties by contacting

financial-privacy@scireat.com. Opt-out requests will be honored within 30 days of receipt;

- **FTC Act Protections:** The Federal Trade Commission Act prohibits unfair or deceptive acts or practices in or affecting commerce. Our data practices are designed to be consistent with FTC guidance on privacy and data security, and we do not engage in practices that would constitute an unfair or deceptive act or practice with respect to the collection, use, or disclosure of Personal Data; and
- **COPPA Protections:** The Children's Online Privacy Protection Act (COPPA) applies to the online collection of Personal Data from children under 13. The Scireat Group does not knowingly collect, use, or disclose Personal Data from children under 13 years of age. If we discover that Personal Data of a child under 13 has been collected without verifiable parental consent, we will promptly delete such data. See Section 13 for our complete Children's Privacy Policy.

12.2 Kansas Residents

Scireat LLC is organized under the laws of Kansas and maintains its principal place of business in Maize, Kansas. Kansas residents have the following rights and protections:

- **Kansas Protection of Consumer Information Act (K.S.A. 50-7a01 through 50-7a04):** Kansas residents have the right to prompt notification, without unreasonable delay, in the event of a security breach affecting their personal information maintained by the Scireat Group. Notice will be provided by the most expedient means possible and will include: a description of the nature of the breach; the categories of personal information involved; the approximate date of the breach; and steps that affected individuals can take to protect themselves. Breach notification inquiries may be directed to privacy@scireat.com;
- **Kansas Consumer Protection Act (K.S.A. 50-623 et seq.):** The Kansas Consumer Protection Act prohibits deceptive and unconscionable acts and

practices in the conduct of trade or commerce. Our data practices are designed to be fully consistent with KCPA requirements, and we do not engage in deceptive practices with respect to the collection, use, or disclosure of Personal Data;

- **Kansas Insurance Department Regulations:** To the extent that Accelavest Financial Services LLC is subject to the regulatory jurisdiction of the Kansas Insurance Department with respect to its financial services activities, it complies with applicable Kansas Insurance Department data privacy regulations governing the protection and use of personal financial information of Kansas insurance customers; and
- **Voluntary Extension of Rights:** The State of Kansas does not currently have a comprehensive consumer data privacy statute comparable to the CCPA/CPRA or GDPR. Nonetheless, Scireat LLC voluntarily extends to all Kansas residents the full suite of data rights described in this Section 12, including the rights of access, deletion, correction, and opt-out described in Sections 12.3 and 12.4, as a matter of company policy and our commitment to privacy as a fundamental value.

12.3 California Residents — CCPA/CPRA

California residents have the following rights under the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, and as supplemented by the regulations of the California Privacy Protection Agency (CPPA) in effect as of the Effective Date of this Privacy Policy:

- **Right to Know:** The right to request that we disclose the categories and specific pieces of Personal Information we have collected about you, the categories of sources from which it was collected, the business or commercial purposes for collection, the categories of third parties to whom it was disclosed, and the categories of Personal Information sold or shared. Pursuant to 2026 CPPA regulations, California residents may request information about Personal Information collected from January 1, 2022, not limited to the preceding 12-month period;

- **Right to Delete:** The right to request deletion of Personal Information we have collected from you, subject to certain exceptions permitted by the CCPA/CPRA, including data necessary to complete a transaction, to comply with a legal obligation, or for security purposes;
- **Right to Correct:** The right to request correction of inaccurate Personal Information maintained about you, subject to verification;
- **Right to Opt-Out of Sale or Sharing:** The Scireat Group does not sell Personal Information. To the extent that our use of analytics or advertising tracking technologies constitutes "sharing" of Personal Information for cross-context behavioral advertising, California residents may opt out by: (a) submitting an opt-out request at scireat.com/privacy-requests; (b) emailing privacy@scireat.com with the subject line "CCPA Opt-Out Request"; or (c) activating the Global Privacy Control signal in a supported browser;
- **Right to Limit Use of Sensitive Personal Information:** California residents have the right to direct the Scireat Group to limit the use of their Sensitive Personal Information to uses necessary to perform the services requested, or as otherwise permitted by CCPA/CPRA Section 1798.121. Requests to limit use of Sensitive Personal Information may be submitted to privacy@scireat.com;
- **Right to Non-Discrimination:** We will not discriminate against you for exercising any of your CCPA/CPRA rights. You will not receive a different level of service, different prices, or a lower quality of goods or services as a result of exercising your privacy rights;
- **Right to Opt-Out of Automated Decision-Making Technology (ADMT):** Effective January 1, 2027, pursuant to the CPPA's 2026 ADMT regulations, California residents have the right to opt out of the Scireat Group's use of automated decision-making technology that produces legal or similarly significant effects concerning you. Prior to January 1, 2027, California residents may request human review of any automated decision as described in Section 7.8;

- **How to Submit a CCPA Request:** Verified CCPA requests may be submitted by email to privacy@scireat.com (subject line: "CCPA Privacy Request") or through our online Privacy Request Portal at scireat.com/privacy-requests. We will verify your identity before processing your request by requiring confirmation of your email address on file and, for requests to know specific pieces of Personal Information or for deletion of Sensitive Personal Information, one additional verification factor;
- **Authorized Agent Requests:** California residents may designate an authorized agent to submit CCPA requests on their behalf. To authorize an agent, you must: (a) provide the Scireat Group with signed written authorization designating the agent; and (b) verify your own identity directly with us. We will not require you to verify your identity directly if you have provided a power of attorney pursuant to California Probate Code Sections 4121–4130;
- **Symmetrical Opt-Out Process:** Consistent with 2026 CPPA design requirement regulations, the number of steps required to opt out of the sale or sharing of Personal Information is equal to or fewer than the number of steps required to opt in to such sale or sharing. Our opt-out mechanisms are designed to be as straightforward as our opt-in processes; and
- **Annual Statistics:** Annual statistics on CCPA/CPRA rights requests received, completed, and denied will be published in our Annual CCPA Report, available at scireat.com/privacy-policy/ccpa-report.

12.4 European Economic Area and UK Residents — GDPR / UK GDPR

Individuals located in the European Economic Area (EEA) and the United Kingdom have the following rights under the General Data Protection Regulation (Regulation (EU) 2016/679) and the UK General Data Protection Regulation (as retained in UK law by the European Union (Withdrawal) Act 2018), respectively:

- **Right of Access (Article 15 GDPR):** The right to obtain confirmation as to whether we process Personal Data concerning you, and if so, to receive a copy of that Personal Data along with supplementary information including

the purposes of processing, the categories of Personal Data, the recipients or categories of recipients, the envisaged retention period, and your rights under the GDPR;

- **Right to Rectification (Article 16 GDPR):** The right to obtain without undue delay the rectification of inaccurate Personal Data concerning you and the completion of incomplete Personal Data;
- **Right to Erasure / Right to be Forgotten (Article 17 GDPR):** The right to obtain deletion of Personal Data concerning you in specified circumstances, including where the data is no longer necessary for the purposes for which it was collected, where you withdraw consent and there is no other lawful basis for processing, or where you object to processing and there are no overriding legitimate grounds;
- **Right to Restriction of Processing (Article 18 GDPR):** The right to obtain restriction of processing in specified circumstances, including where you contest the accuracy of the data, where processing is unlawful and you oppose erasure, or where you have objected to processing pending verification of whether our legitimate grounds override your interests;
- **Right to Data Portability (Article 20 GDPR):** Where processing is based on consent or on a contract and is carried out by automated means, the right to receive your Personal Data in a structured, commonly used, and machine-readable format and to transmit it to another controller;
- **Right to Object (Article 21 GDPR):** The right to object at any time to processing of your Personal Data on grounds of our legitimate interests (Article 6(1)(f)), including profiling based on those interests. We will cease processing unless we demonstrate compelling legitimate grounds that override your interests, rights, and freedoms, or for the establishment, exercise, or defense of legal claims. You have an unconditional right to object to processing for direct marketing purposes;
- **Rights Related to Automated Decision-Making and Profiling (Article 22 GDPR):** The right not to be subject to a decision based solely on

automated processing, including profiling, which produces legal or similarly significant effects concerning you, except in specified circumstances. Where such processing occurs, you have the right to request human intervention, to express your point of view, and to contest the decision;

- **Right to Lodge a Complaint:** The right to lodge a complaint with the supervisory authority of your EU member state of habitual residence, place of work, or place of the alleged infringement, or with the Information Commissioner's Office (ICO) in the United Kingdom;
- **Data Controller Contact:** Scireat LLC, Privacy Officer, Maize, Kansas, United States; privacy@scireat.com;
- **EU/UK Representative:** Where required by GDPR Article 27 or UK GDPR Article 27, Scireat LLC will appoint an EU and/or UK representative. Information about our designated representative(s), if applicable, will be published at scireat.com/privacy-policy;
- **Data Protection Officer:** Scireat LLC has designated a Data Protection Officer (DPO) reachable at dpo@scireat.com for matters relating to GDPR compliance; and
- **Response Timeline:** We will respond to verified GDPR rights requests within 30 calendar days of receipt. Where the complexity or number of requests requires additional time, we may extend the response period by up to 60 additional calendar days (for a total of 90 calendar days), provided that we notify you of the extension and the reasons for it within the initial 30-day period.

12.5 How to Exercise Your Rights

Individuals may exercise any of the rights described in this Section 12 through the following channels:

- **Email:** privacy@scireat.com — Please include your full name, the email address associated with your account (if applicable), your jurisdiction of residence, and a clear description of the right you wish to exercise;

- **Online Privacy Request Portal:** scireat.com/privacy-requests — A guided request submission form that allows you to select the type of request and provide the required information;
- **Mail:** Scireat LLC, Privacy Officer, Maize, Kansas, United States — Please provide the same information as required for email requests; and
- **For Accelavest Financial Services LLC GLBA opt-out requests:** financial-privacy@scireat.com.

Response Timelines: Kansas and other U.S. residents (voluntary): 45 calendar days, extendable by 45 days with notice. California residents (CCPA/CPRA): 45 calendar days, extendable by 45 calendar days with notice. EEA/UK residents (GDPR): 30 calendar days, extendable by 60 days for complex requests with notice. We will acknowledge receipt of all requests within 5 business days.

Identity Verification: To protect the security of Personal Data, we verify the identity of requesters before processing rights requests. Standard verification requires confirmation of the email address on file. Requests for specific pieces of Sensitive Personal Information or deletion requests require one additional verification factor, which may include verification of a secondary contact method, answers to security questions, or provision of a government-issued identifier for matching purposes only. We will not use information provided for identity verification for any other purpose.

13. CHILDREN'S PRIVACY

The Scireat Group does not knowingly collect, use, maintain, or disclose Personal Information from children under the age of 13, and our services are not directed to children under 13. The IncomeCompliant platform is designed for use by individuals who are at least 18 years of age, and all Scireat Group services other than the IncomeCompliant platform are directed to adults. We do not knowingly solicit Personal Information from children under 13 or market to children under 13.

If we become aware that we have inadvertently collected Personal Information from a child under 13 without verifiable parental consent as required by the Children's

Online Privacy Protection Act (15 U.S.C. § 6501 et seq.) and its implementing regulations (16 C.F.R. Part 312), we will take the following steps promptly upon discovery: (a) cease collection of any additional Personal Information from the child; (b) delete all Personal Information collected from the child from our systems, subject only to any retention required by law; (c) notify the parent or legal guardian of the child if their contact information is available; and (d) document the incident in our internal incident log.

Parents or legal guardians who believe that the Scireat Group has collected Personal Information from their child under 13 without their consent are urged to contact us immediately at privacy@scireat.com or by mail at Scireat LLC, Privacy Officer, Maize, Kansas, United States. We will investigate and respond to such inquiries within 15 business days.

14. THIRD-PARTY LINKS AND INTEGRATIONS

Our websites, the IncomeCompliant platform, and other Scireat Group services may contain links to, or enable integrations with, third-party websites, applications, and services that are not owned or operated by the Scireat Group. These third-party sites and services are governed by their own privacy policies and terms of service, and the Scireat Group is not responsible for the privacy practices, security measures, or data handling procedures of any third party. The inclusion of a link or integration in a Scireat Group service does not constitute an endorsement of the third party's privacy practices.

Users of the IncomeCompliant platform may connect the platform with third-party services, including payroll processors, banking institutions via open banking APIs, tax preparation software, and benefits administration platforms. When you authorize such connections, you are directing the Scireat Group to exchange data with the third-party service on your behalf, and you are also subject to the third party's privacy policy and terms of service with respect to that third party's own use of your data. We strongly encourage users to review the privacy policies of all integration partners before authorizing a connection. A list of supported integration partners

and links to their privacy policies is maintained in the IncomeCompliant platform's integration marketplace documentation.

The Scireat Group does not receive any compensation from integration partners based on the collection or use of user Personal Data transmitted through platform integrations. Integration partners are contractually prohibited from using Personal Data received through IncomeCompliant integrations for any purpose other than providing the authorized service to the user.

15. CHANGES TO THIS PRIVACY POLICY

The Scireat Group reviews this Privacy Policy on an ongoing basis and reserves the right to update or modify it at any time to reflect changes in our data practices, the services we offer, applicable law, or regulatory requirements. Changes to this Privacy Policy are classified as either material or non-material.

Material Changes: A change is material if it alters the categories of Personal Data we collect, the purposes for which we use Personal Data, the circumstances under which we share Personal Data with third parties, or the rights available to individuals in a way that is adverse to or significantly different from the existing provisions of this Privacy Policy. For material changes, we will provide not less than 30 calendar days' advance written notice to all registered users by email to the address on file and by prominent in-application notification within the IncomeCompliant platform and Scireat Group websites before the changes take effect. Enterprise customers will additionally receive notice through their designated account contacts.

Non-Material Changes: Changes that do not materially affect individuals' rights or the Scireat Group's core data practices — such as clarifications, corrections of typographical errors, or updates to contact information — will be posted with an updated Effective Date on the Scireat Group's privacy policy page without prior notice.

Acceptance: Continued use of any Scireat Group service after the notified effective date of material changes constitutes acceptance of the updated Privacy Policy. If you

do not agree with the changes, you should cease using our services and may request deletion of your Personal Data as described in Section 12.5 before the changes take effect.

Version History: A complete version history of this Privacy Policy, including prior versions in full text and a summary of changes between versions, is maintained and publicly available at scireat.com/privacy-policy/history.

16. CONTACT INFORMATION AND DATA CONTROLLER DETAILS

Data	Controller	and	Holding	Company:
		Scireat		LLC
	Maize,	Kansas,	United	States
	General	Inquiries:		info@scireat.com
	Privacy	Officer:		privacy@scireat.com

Data Protection Officer (GDPR): dpo@scireat.com

Privacy Officer — All Privacy Rights Requests and Inquiries:
Email: privacy@scireat.com

Online Portal: scireat.com/privacy-requests

Mail: Scireat LLC, Privacy Officer, Maize, Kansas, United States

Accelavest Financial Services LLC — GLBA and Financial Privacy Inquiries:

Email: financial-privacy@scireat.com

Data Protection Officer — GDPR and UK GDPR Matters:

Email: dpo@scireat.com

Response Commitment: The Scireat Group will acknowledge receipt of all privacy inquiries and rights requests within 5 business days of receipt. We will provide a substantive response within the timeframe required by applicable law as specified in Section 12.5, and we will communicate proactively if additional time is required to fulfill a complex request.

For media and press inquiries relating to privacy matters, please contact info@scireat.com with the subject line "Privacy Media Inquiry."

17. REGULATORY COMPLIANCE SUMMARY TABLE

The following table provides a summary of the primary legal and regulatory frameworks that govern the Scireat Group's data processing activities, the jurisdictions and populations covered, the primary rights those frameworks afford to individuals, the Scireat Group's principal obligations under each framework, and the relevant contact point within the Scireat Group.

Law / Framework	Jurisdiction / Population Covered	Primary Rights Granted to Individuals	Scireat Group's Principal Obligations	Scireat Contact Point
Gramm-Leach-Bliley Act (GLBA) 15 U.S.C. §§ 6801–6809; 16 C.F.R. Part 314	U.S. customers of Accelavest Financial Services LLC	Annual privacy notice; right to opt out of certain NPI sharing with non-affiliated third parties	Deliver annual privacy notice; maintain written information security program (WISP) per FTC Safeguards Rule; honor opt-out requests within 30 days	financial-privacy@scireat.com
FTC Act 15 U.S.C. § 45	All U.S. consumers	Protection against unfair or deceptive acts or practices in data collection and use	Maintain accurate and non-deceptive privacy disclosures; honor stated privacy commitments; maintain reasonable security practices	privacy@scireat.com
COPPA 15 U.S.C. § 6501	Children under 13 in	Parental consent	Do not knowingly	privacy@scireat.com

Law / Framework	Jurisdiction / Population Covered	Primary Rights Granted to Individuals	Scireat Group's Principal Obligations	Scireat Contact Point
et seq.; 16 C.F.R. Part 312	the United States	required before collection; right of parents to review, delete, and refuse further collection of child's data	collect personal information from children under 13 without verifiable parental consent; delete upon discovery; notify parents	
HIPAA / HITECH 45 C.F.R. Parts 160, 162, 164 (BAA contexts only)	U.S. individuals whose PHI is processed pursuant to a BAA with a Covered Entity	Access, amendment, accounting of disclosures, restriction of processing (in BAA contexts); HIPAA-equivalent rights extended voluntarily to all Health-Financial Data subjects	Execute BAAs before PHI flows; apply Minimum Necessary standard; maintain HIPAA Security Rule-equivalent technical safeguards; report breaches per HITECH/BAA terms	privacy@scireat.com
FTC Health Breach Notification Rule 16 C.F.R. Part 318 (as amended 2024)	U.S. individuals whose personal health records are processed by non-HIPAA-covered health apps or services	Right to notification within 60 days of breach discovery	Notify affected individuals, FTC, and (for breaches ≥500 individuals) prominent state media within 60 days of breach discovery	privacy@scireat.com
Kansas Protection of Consumer Information Act K.S.A. 50-7a01 through 50-7a04	Kansas residents	Right to prompt, non-delayed notification of a security breach affecting their	Notify affected Kansas residents of security breaches without unreasonable	privacy@scireat.com

Law / Framework	Jurisdiction / Population Covered	Primary Rights Granted to Individuals	Scireat Group's Principal Obligations	Scireat Contact Point
		personal information	delay; provide required breach notification content	
CCPA / CPRA Cal. Civil Code §§ 1798.100–1798.199.100; 2026 CPPA Regulations	California residents	Know; Delete; Correct; Opt-Out of Sale/Sharing; Limit SPI; Non-Discrimination ; Opt-Out of ADMT (eff. Jan. 1, 2027)	Honor verified consumer rights requests within 45 days (+45 extension); maintain compliant privacy notice; implement symmetrical opt-out; publish annual statistics; honor GPC signals	privacy@scireat.com; scireat.com/privacy-requests
GDPR (EU) Regulation (EU) 2016/679	EEA residents and individuals whose data is processed by Scireat Group in the context of offering services to EEA residents	Access (Art. 15); Rectification (Art. 16); Erasure (Art. 17); Restriction (Art. 18); Portability (Art. 20); Object (Art. 21); ADMT rights (Art. 22); Lodge complaint with supervisory authority	Establish lawful basis for processing; honor DSARs within 30 days (+60 extension); maintain records of processing; implement SCCs or other transfer mechanisms; appoint DPO; conduct DPIAs for high-risk processing	dpo@scireat.com; privacy@scireat.com
UK GDPR UK GDPR as retained by EU (Withdrawal)	UK residents and individuals whose data is processed by	Same rights as GDPR (EU); right to lodge complaint with UK ICO	Same obligations as GDPR (EU); use UK IDTA or UK	dpo@scireat.com; privacy@scireat.com

Law / Framework	Jurisdiction / Population Covered	Primary Rights Granted to Individuals	Scireat Group's Principal Obligations	Scireat Contact Point
Act 2018; Data Protection Act 2018	Scireat Group in the context of offering services to UK residents		Addendum to SCCs for international transfers; honor ICO guidance; appoint UK representative if required	

ATTESTATION AND APPROVAL

This Privacy Policy was reviewed and approved by the Scireat LLC Privacy Officer and authorized by Scireat LLC management as of the Effective Date set forth herein. This document constitutes the authoritative, publication-ready Privacy Policy of Scireat LLC and the Scireat Group, effective September 13, 2026, superseding all prior privacy policies, privacy notices, and data processing statements issued by Scireat LLC or any member of the Scireat Group in their entirety.

Privacy Officer, Scireat LLC

Signature

Date: September 13, 2026

Authorized Representative, Scireat LLC Management

Signature

Date: September 13, 2026

Scireat LLC — Maize, Kansas, United States | privacy@scireat.com | scireat.com/privacy-policy

Privacy Policy v2.0 | Effective Date: September 13, 2026 | Version History: scireat.com/privacy-policy/history

© 2026 Scireat LLC. All rights reserved. This document is the property of Scireat LLC and may not be reproduced or distributed without written authorization.