

FIRST-PARTY PRIVACY POLICY - INTERVAL AI CORPORATION

Effective Date: August 7, 2026

This First-Party Privacy Policy (the **Policy**) explains how Interval AI Corporation (**Interval, we, us, or our**) collects, uses, discloses, and retains personal information through interval-ai.com and any website, landing page, dashboard, portal, application, or other digital service that links to this Policy (collectively, the **Online Services**), and in connection with first-party account outreach and related services provided for Interval's business customers (the **Services**).

Interval's address is 356 S 2000 W, Suite A, Pleasant Grove, Utah 84062. Privacy questions and requests may be submitted to support@interval-ai.com.

1. SCOPE AND OUR ROLES

This Policy applies to information about our customers and their personnel, prospective customers, website visitors, Online Services users, and individuals whose accounts or obligations are serviced through Interval on behalf of a customer.

For customer-provided consumer information and customer-directed outreach, Interval generally acts as a service provider or processor on behalf of the customer. The customer remains responsible for its underlying products, services, accounts, notices, consents, instructions, and relationship with the individual. Interval may act as an independent business or controller for its own website operations, security, fraud prevention, legal compliance, billing, analytics, service evaluation, model and workflow improvement, corporate administration, and other purposes described in this Policy, subject to applicable agreements and law.

This Policy does not replace a customer's privacy notice. If you were contacted about an account held by one of our customers, that customer's notice may also apply. A signed data processing agreement or other customer agreement may control if it expressly conflicts with this Policy for the processing it covers.

2. INFORMATION WE COLLECT

We may collect the following categories of information.

2.1 Identifiers and Contact Information

Names, aliases, postal addresses, email addresses, telephone numbers, customer and account identifiers, usernames, IP addresses, device identifiers, and similar identifiers.

2.2 Customer and Professional Information

Business names, job titles, departments, work contact details, authorized-user status, login information, contracts, subscription details, service configurations, support history, billing contacts, and information about a customer's operations and use of the Services.

2.3 Consumer Account and Transaction Information

Account balances, invoice information, products or services purchased, service and transaction dates, amounts owed, credits, refunds, payment history, delinquency status, account notes, relevant contracts, supporting records, and customer instructions.

2.4 Payment Information

Payment method, tokenized card or bank information, transaction status, payment history, authorization records, recurring-payment instructions, receipts, processor responses, returned payments, chargebacks, and fraud indicators. Complete card and bank credentials are generally handled through approved secure interfaces and PCI-compliant processors. Interval may retain payment tokens, last four digits, bank name, status, authorization records, and other information needed to administer transactions.

2.5 Communications and Preferences

Calls, recordings, transcripts, voicemail, text messages, email, webchat, support interactions, dispute-center submissions, communication content, consent and opt-out records, preferred channels, convenient or inconvenient times and places, language preferences, complaints, and interactions with AI or human representatives.

The dispute center does not currently permit document uploads. Do not attempt to transmit documents or highly sensitive information through an unapproved channel.

2.6 Dispute, Hardship, and Compliance Information

Disputes, service or cancellation issues, hardship information, bankruptcy information, attorney representation, identity-theft reports, fraud concerns, complaints, payment-plan requests, settlement requests, and information needed for human review, escalation, or compliance.

2.7 Internet, Device, and Usage Information

Browser type, operating system, device settings, cookie and advertising identifiers, pages viewed, links selected, referring pages, approximate location inferred from IP address, session activity, login attempts, feature usage, diagnostics, error logs, performance data, and security events.

2.8 Marketing and Prospect Information

Contact information, company information, campaign engagement, event participation, form submissions, advertising interactions, lead source, communications, meeting information, and inferred interest in Interval's products or services.

2.9 Sensitive Information

Interval does not ordinarily require Social Security numbers, government identification numbers, dates of birth, complete payment credentials, medical records, protected health information, or similar highly sensitive information for the Services. We may receive sensitive information incidentally or when reasonably necessary and lawful. Such information must be transmitted only through encryption or another Interval-approved secure method and only when specifically requested or authorized.

Ordinary email, text messaging, and webchat may not be secure. Do not send complete card numbers, bank credentials, Social Security numbers, government identification, medical records, detailed treatment information, passwords, or other highly sensitive information through those channels.

2.10 Inferences and Derived Information

Account categorization, communication recommendations, likely channel or timing preferences, engagement indicators, quality scores, fraud or security indicators, product interests, workflow recommendations, model outputs, and other inferences derived from the information described above.

3. SOURCES OF INFORMATION

We may receive information from:

- Customers, their authorized users, affiliates, processors, and service providers.
- Consumers, account holders, representatives, attorneys, and other individuals who communicate with us or our customers.
- Payment processors, banks, card networks, communications providers, identity-verification services, fraud-prevention services, and integration partners.
- Public records, publicly available sources, data providers, enrichment services, and other lawful third-party sources.
- Devices, browsers, cookies, pixels, analytics tools, session and interaction tools, logs, and security technologies.

- Interval affiliates, vendors, professional advisors, referral sources, advertising partners, and business partners.

Information received from customers or other third parties may be inaccurate, incomplete, or outdated. Contact us or the relevant customer if you believe information about you is incorrect.

4. HOW WE USE INFORMATION

We may use personal information to:

- Provide, configure, administer, support, secure, and improve the Services and Online Services.
- Authenticate users, manage permissions, maintain accounts, and prevent unauthorized access.
- Conduct first-party outreach on behalf of customers concerning accounts, balances, invoices, payments, service issues, and related matters.
- Generate and deliver calls, text messages, email, webchat, recordings, transcripts, and other communications.
- Process, facilitate, reconcile, reverse, and document payments, payment plans, settlements, refunds, chargebacks, and related transactions.
- Receive, route, investigate, document, and help resolve disputes, hardships, cancellation requests, complaints, bankruptcy matters, attorney representation, identity theft, and other escalations.
- Apply communication preferences, consent records, suppression rules, timing controls, and customer-approved outreach parameters.
- Provide recommendations concerning timing, tone, cadence, channel, payment arrangements, settlements, and next actions.
- Perform analytics, testing, evaluation, quality assurance, training, research, model improvement, workflow development, and product improvement.
- Aggregate, deidentify, minimize, or otherwise transform information where practical.
- Detect and prevent fraud, misuse, security incidents, unauthorized activity, and other unlawful conduct.
- Monitor performance, diagnose errors, maintain backups, and support business continuity.
- Invoice customers, administer contracts, enforce agreements, collect amounts owed to Interval, and maintain business records.
- Comply with laws, subpoenas, court orders, audits, regulatory requests, sanctions, and recordkeeping duties.
- Establish, exercise, or defend legal claims; protect Interval, our customers, individuals, and others; and support corporate governance, financing, insurance, diligence, transactions, and reorganizations.
- Market Interval's products and services, measure campaigns, personalize public website experiences, and conduct targeted advertising as described below.

5. FIRST-PARTY OUTREACH, AI, AND HUMAN REVIEW

Interval provides technology and related services that allow customers to communicate about their own accounts. Communications are generally made on behalf of and under the identity of the relevant customer, although Interval may identify itself when appropriate or required.

We may use artificial intelligence, machine learning, language models, synthesized speech, open-source models, and automated decision-support tools. An AI or virtual assistant will identify itself during initial outreach and when asked, subject to channel limitations and applicable law. AI output may contain errors, delays, or incomplete information.

Interval may recommend outreach timing, tone, cadence, channel, payment arrangements, settlements, or other actions. Customers provide final approval or establish approved rules and parameters. Certain matters may be paused or routed for human review, including disputes, hardship, cancellation requests, service disputes, bankruptcy, attorney representation, fraud concerns, and other escalations. Interval personnel or a customer's live agent may review or take over an interaction.

Communications may be recorded or transcribed where permitted and with any notice or consent required by law.

6. AI TRAINING AND PRODUCT IMPROVEMENT

Interval may use identifiable customer and consumer information across its systems, products, and customer base where reasonably necessary and permitted by contract and law for security, compliance, fraud prevention, error investigation, service operation, quality assurance, evaluation, training, model improvement, workflow development, analytics, research, and product improvement.

We may use recordings, transcripts, interaction outcomes, payment behavior, account events, disputes, workflow results, and user feedback for these purposes. Where practical, Interval may aggregate, deidentify, minimize, pseudonymize, or otherwise transform information. Interval will not attempt to reidentify information that has been properly deidentified except to test or validate deidentification, improve security, comply with law, or as otherwise permitted by law.

Interval independently determines certain purposes and methods for its security, compliance, evaluation, training, analytics, and product-improvement activities, subject to applicable customer agreements and law. Customers authorize the processing described in this Policy when they provide information to Interval or use the Services.

Service providers may process information to provide technology and services to Interval, but they are not authorized by Interval to use customer or consumer information to train their own independent models.

7. HOW WE DISCLOSE INFORMATION

We may disclose personal information to the following categories of recipients for the purposes described in this Policy.

7.1 Customers and Authorized Account Participants

The customer on whose behalf Interval provides Services, the customer's authorized users and affiliates, and persons the customer authorizes to receive information. Customers are responsible for their own use and disclosure of information.

7.2 Service Providers and Technology Vendors

Database, hosting, cloud, telephony, messaging, email, artificial-intelligence, transcription, analytics, error-logging, security, identity-verification, payment, compliance, registration, customer-support, and professional-service providers. Current providers may include Supabase, OpenAI, Telnyx, PostHog, Campaign Registry, Google, Meta, Microsoft Clarity, payment processors, and open-source model infrastructure. Providers may change without an amendment to this Policy.

7.3 Payment and Financial Participants

Payment processors, banks, card networks, digital-wallet providers, account owners, and other entities involved in authorizing, processing, settling, reconciling, reversing, or investigating a transaction.

7.4 Legal, Safety, and Compliance Recipients

Regulators, courts, law enforcement, government agencies, auditors, insurers, attorneys, advisors, and other parties when required or reasonably necessary to comply with law, respond to legal process, protect rights or safety, investigate misconduct, enforce agreements, or establish or defend claims.

7.5 Corporate Transactions and Affiliates

Interval affiliates, investors, lenders, insurers, advisors, and actual or potential buyers, successors, or transaction counterparties in connection with financing, diligence, insurance, merger, acquisition, reorganization, bankruptcy, or sale of assets, subject to appropriate protections.

7.6 At Your Direction or With Consent

Persons you direct us to contact or whom you authorize to receive information, and other recipients with your consent or at your direction.

We may disclose aggregated or deidentified information that cannot reasonably be linked to an identifiable person, subject to applicable law.

8. COOKIES, ANALYTICS, AND SESSION TECHNOLOGIES

We may use cookies, pixels, local storage, tags, software development kits, session-replay tools, interaction tools, and similar technologies on public websites and landing pages to:

- Operate the website and remember settings.
- Authenticate users and maintain security.
- Measure traffic, engagement, conversions, and campaign performance.
- Diagnose errors and improve design, content, and usability.
- Personalize public website experiences.
- Support advertising and targeted advertising.

Tools may include Google Analytics, Google advertising technologies, Meta Pixel, Microsoft Clarity, PostHog, and similar services. These providers may receive online identifiers, IP addresses, device and browser information, referring pages, page activity, interaction data, and advertising or conversion events.

Advertising pixels and session-replay tools may operate across our Online Services, including on authenticated dashboards, payment pages, dispute-center pages, account-specific pages, and pages that display customer or consumer account information. These tools may capture information entered into or displayed on those pages, including account, payment, and other potentially sensitive information, and input fields are not necessarily masked or excluded from session recording. If you have questions about how these technologies operate or the information they may capture, contact support@interval-ai.com.

Where required, nonessential cookies and similar technologies will not be activated until you make a choice through our cookie banner or preference tool. Browser settings may also block or delete cookies, but doing so may impair features.

9. TARGETED ADVERTISING AND PRIVACY CHOICES

Interval does not sell personal information for money. We may disclose website identifiers and public website activity to advertising partners such as Google and Meta to measure advertising, create audiences, and provide targeted advertising. These disclosures may be treated as a sale, sharing, or targeted-advertising processing under certain privacy laws even though Interval does not receive money for the information.

Interval does not use or disclose customer account data, balances, invoices, disputes, payment information, first-party outreach communications, recordings, transcripts, dispute-center information, or consumer account activity for targeted advertising.

Where applicable, you may opt out of targeted advertising and the sale or sharing of personal information by using the **Your Privacy Choices** link or emailing support@interval-ai.com. We will honor qualifying browser-based opt-out preference signals, such as Global Privacy Control, as required by law. A browser signal generally applies to the browser or device sending it. We may request additional information if you want an opt-out associated with an account and the law permits that request.

10. COMMUNICATION PREFERENCES

You may request changes to marketing communications by using an unsubscribe link or contacting support@interval-ai.com. You may communicate channel, number, email, time, place, language, or other preferences for account outreach through the method provided in the communication, through the relevant customer, or by contacting support.

Replying STOP to a text message ordinarily stops further messages of that type to the relevant number. A channel opt-out does not necessarily prevent legally permitted or requested communications through another channel and does not cancel an account, payment authorization, contract, or legal obligation.

Communication preferences and marketing opt-outs are separate from formal privacy requests. We may retain suppression records to honor an opt-out.

11. PAYMENT SECURITY

Interval is PCI compliant and uses PCI-compliant payment processors and practices. Complete card and bank credentials should be entered only through an approved secure payment interface. Do not send complete payment credentials through ordinary email, text, or webchat.

No payment system, processor, bank, carrier, or network is completely secure or continuously available. Interval does not control every third-party processor or financial institution and cannot guarantee that a transaction will be authorized, settled, uninterrupted, or error-free.

12. HEALTH AND OTHER HIGHLY SENSITIVE INFORMATION

Services for healthcare customers may involve limited patient billing information, such as a responsible party's name, contact information, and balance. Customers must not provide medical records, diagnoses, treatment details, or protected health information unless Interval has expressly approved the data, the disclosure is lawful, a secure method is used, and the parties have completed any agreement required by law.

Unless a signed agreement expressly states otherwise, use of the Services does not make Interval a business associate under HIPAA and does not constitute Interval's agreement to receive protected health information. Interval may reject, restrict, return, isolate, or delete improperly submitted sensitive information when permitted, but is not responsible for a customer's failure to identify, minimize, secure, or lawfully disclose that information.

13. CHILDREN

The Online Services and Services are not directed to children under eighteen (18), and Interval does not knowingly collect personal information directly from children. Customers must not submit an account for a minor or provide a minor's information.

If Interval learns that it received a minor's information contrary to this Policy, it may suspend processing and delete, return, restrict, or otherwise remove the information as appropriate and permitted by law. Contact support@interval-ai.com if you believe a minor's information was submitted.

14. DATA SECURITY

Interval uses commercially reasonable administrative, technical, and physical safeguards designed to protect personal information. Measures may include encryption in transit and at rest, access controls, authentication, logging, monitoring, vendor review, incident response, backups, employee confidentiality obligations, and security testing. Interval maintains a SOC 2 Type II program and is PCI compliant.

No method of transmission or storage is completely secure. Interval cannot guarantee that unauthorized access, loss, misuse, alteration, interruption, or other security events will never occur. You are

responsible for protecting credentials, secure links, devices, and networks and for promptly reporting suspected unauthorized activity.

15. DATA RETENTION

Interval generally retains customer account, consumer account, outreach, communication, recording, consent, payment, dispute, security, and compliance records for at least six (6) years after the relevant account is closed or the customer relationship ends. We may retain information longer when reasonably needed for law, audits, litigation, disputes, fraud prevention, security, backup integrity, enforcement, model governance, product integrity, or legitimate business records.

Retention periods for cookies, advertising identifiers, analytics data, session data, ordinary website logs, and marketing information may be shorter and may depend on provider settings, consent choices, account status, security needs, and applicable law. Backup copies may remain until overwritten under ordinary cycles.

A deletion request does not require deletion when retention is permitted or required. Interval may delete information when permitted by law, contractual commitments, and its retention practices.

16. YOUR PRIVACY RIGHTS

Depending on your residence, relationship with Interval, the information, and applicable law, you may have rights to:

- Confirm whether we process your personal information and obtain access to it.
- Request correction of inaccurate personal information.
- Request deletion, subject to legal, contractual, security, and operational exceptions.
- Obtain a portable copy of certain information.
- Opt out of sale, sharing, targeted advertising, or certain profiling.
- Limit certain uses or disclosures of sensitive personal information.
- Withdraw consent where processing is based on consent.
- Object to or restrict certain processing.
- Appeal a denial of a privacy request.
- Receive information about categories of data, sources, purposes, and recipients.
- Complain to an applicable privacy or data-protection authority.

These privacy rights are separate from billing, account, cancellation, dispute, payment, and communication rights. A privacy request does not automatically dispute, cancel, settle, validate, or delete an account or accurate business record.

16.1 Submitting a Request

Submit a request to support@interval-ai.com. Describe the right you wish to exercise and provide enough information for us to identify the relevant records. Do not email highly sensitive documents unless we provide an approved secure method.

16.2 Verification

We may verify identity and authority using information already associated with you, such as contact information, customer relationship, account reference, address, or secure authentication. We may deny or limit a request if we cannot reasonably verify identity or authority, an exemption applies, the request is excessive or fraudulent, retention is permitted or required, or fulfilling the request would violate another person's rights, a customer agreement, or applicable law.

16.3 Customer-Controlled Information

If Interval processes information solely on behalf of a customer, we may refer the request to that customer or assist the customer in responding. The customer may be responsible for deciding the request. Contacting Interval does not relieve the customer of its obligations.

16.4 Authorized Agents and Appeals

Where permitted, an authorized agent may submit a request. We may require proof of authorization and direct identity verification. If applicable law provides an appeal right, reply to our decision or email support@interval-ai.com with the subject **Privacy Appeal** and explain the basis for appeal.

16.5 Nondiscrimination

Interval will not unlawfully discriminate against you for exercising a privacy right. Exercising a right may affect functionality where the information is necessary for authentication, security, payments, account servicing, compliance, fraud prevention, or another permitted purpose.

17. U.S. STATE PRIVACY DISCLOSURES

For residents of states with comprehensive privacy laws, personal information collected during the preceding twelve months may include identifiers; customer records; commercial, transaction, professional, internet, audio, electronic, payment, and sensitive information; and inferences. The sources, business and commercial purposes, and categories of recipients are described in Sections 3, 4, and 7.

Interval does not sell personal information for money. Interval may share public website identifiers and activity with advertising partners for cross-context behavioral or targeted advertising as described in Section 9. Depending on applicable law, you may opt out through **Your Privacy Choices**, a qualifying browser signal, or support@interval-ai.com.

We use and disclose sensitive personal information only for the Services, authentication, payments, security, compliance, fraud prevention, legal obligations, and other permitted purposes. We do not use sensitive personal information to infer characteristics for advertising.

Some information processed in a business-to-business, employment, financial, healthcare, credit, legal, or regulated context may be exempt from a state privacy law. We will apply the law governing the particular information and request.

18. INTERNATIONAL INFORMATION AND RIGHTS

Interval may provide Services in the United States and other countries. Personal information may be processed in the United States and other locations where Interval or its providers operate. Those locations may have data-protection laws that differ from the laws where you live.

Where required, Interval or the relevant customer will use an approved transfer mechanism and provide additional notices. Lawful bases for processing may include performance of a contract, steps requested before a contract, compliance with legal obligations, legitimate interests in providing and improving the Services, security, fraud prevention, account administration, establishment or defense of legal claims, and consent.

Individuals in certain jurisdictions may have rights to access, correct, delete, restrict, object, withdraw consent, request portability, receive information about transfer safeguards, or complain to a supervisory authority. Contact support@interval-ai.com to exercise applicable rights.

19. THIRD-PARTY SERVICES AND LINKS

The Online Services may link to or integrate with customer websites, payment processors, communications providers, social networks, and other third-party services. Their privacy practices are governed by their own notices. Interval is not responsible for third-party services outside its control.

20. CHANGES TO THIS POLICY

We may update this Policy to reflect legal, operational, vendor, technology, or service changes. The effective date above identifies the current version. We will provide additional notice of material changes when required by law. Prior versions may be retained for compliance and business records.

21. CONTACT US

INTERVAL AI CORPORATION

356 S 2000 W, Suite A

Pleasant Grove, Utah 84062

support@interval-ai.com

interval-ai.com