Privacy Policy

Bleedpoint Revenue Audit Service

Service Provider: Bleedpoint (a product of CloudSec Global LLC) **Document Version:** 0.9 **Effective Date:** April 26, 2026

1. Introduction

This Privacy Policy explains how Bleedpoint collects, uses, stores, and shares personal data when you use our revenue audit service. We've tried to write it in plain English, with the legal precision necessary to protect your rights and ours.

If you have questions after reading this, email us at hello@bleedpoint.com or legal@bleedpoint.com.

1.1 Who We Are

Bleedpoint is a product of **CloudSec Global LLC**, a Nevada limited liability company. For the purposes of this policy:

- **"We," "us," "our," "Bleedpoint":** CloudSec Global LLC operating the Bleedpoint service
- **"You," "your":** the person or entity using Bleedpoint
- **"Personal data":** information that identifies or can reasonably be linked to an identifiable person
- **"Service":** the Bleedpoint website, web application, audit reports, and related features

1.2 Scope

This policy applies to:

- Visitors to bleedpoint.com (and subdomains)
- Bleedpoint customers (paid and free preview users)
- People whose data flows through our service because the customer connected a billing platform we audit (your customers' data)

It does not apply to:

- Third-party sites we link to (Stripe, AWS, etc. — they have their own policies)
- Data your billing platform handles directly (e.g., card numbers, which never reach us)

2. Data We Collect

We separate the data we collect into two clear categories: **data about you (the customer)** and **data flowing through our service from your billing platform** (which may include personal data about your customers).

2.1 Data About You (the Bleedpoint Customer)

When you sign up and use Bleedpoint, we collect:

Account information:

- Email address (required for authentication)
- Account creation timestamp
- Authentication events (magic link requests, login times, IP addresses)

Billing information:

- Name, billing email, and address (collected by Stripe Checkout, shared back to us)
- Payment method information is processed by Stripe and never stored on Bleedpoint systems
- Transaction history (audit purchases, monthly subscription status)
- Refund requests and their resolution

Usage information:

- Pages visited, features used, audit runs initiated
- Browser type, device type, screen resolution
- IP address and approximate geographic location (city/region level)
- Timestamps of significant actions

Support and communication:

- Email correspondence with our team
- Refund request emails sent to guarantee@bleedpoint.com
- Security disclosures sent to security@bleedpoint.com

2.2 Data Flowing Through Our Service (Your Billing Platform Data)

When you authorize Bleedpoint to access your billing platform via OAuth, we receive data about your business operations and your customers. Depending on your platform and account, this may include:

- Your customers' email addresses, names (if available), and creation dates
- Subscription status, plans, and billing history
- Payment records: amounts, currencies, success/failure status, retry attempts
- Invoice records: amounts, dates, payment status
- Coupon and discount records
- Plan and pricing definitions

What we explicitly do NOT receive:

- Credit card numbers or any payment credentials
- Bank account numbers

- Tax identification numbers (SSN, EIN, etc.) of your customers
- Authentication credentials of any kind
- Content of files, emails, or other application data unrelated to billing

We process this data on your behalf to deliver audit findings. You are the data controller for your customers' data; we are the data processor. Our processing is governed by these Terms and the separate Data Processing Agreement (DPA).

2.3 Cookies and Tracking

Bleedpoint uses a limited set of cookies and tracking technologies. We use CookieYes as our consent management platform to handle cookie preferences and consent records.

Strictly necessary (always active):

- Authentication session cookies (httpOnly, secure, SameSite=Lax) — required for you to stay logged in
- CSRF protection tokens — required to prevent attack attempts
- Consent preference cookies (set by CookieYes) — required to remember your cookie choices

Analytics (with consent where required):

- Google Analytics 4 — usage patterns and aggregate behavior
- Microsoft Clarity — session replay and heatmaps (anonymized, no input field recording)

In jurisdictions that require prior consent (EU, UK, certain others), our consent banner blocks non-essential cookies until you opt in. You can change your preferences at any time via the consent banner or our cookie preference link in the site footer.

We do not use cookies for advertising, do not sell cookie data to third parties, and do not participate in cross-site tracking networks.

3. How We Use Data

3.1 Data About You (the Customer)

We use your personal data to:

- **Provide the service:** authenticate you, run audits, deliver reports, manage your subscription
- **Bill you:** process payments via Stripe, issue refunds when applicable, send receipts
- **Communicate with you:** transactional email (audit-ready notifications, billing receipts, security alerts), respond to support requests
- **Improve the service:** analyze aggregate usage patterns, debug issues, identify product improvements
- **Maintain security:** detect and prevent fraud, abuse, and unauthorized access

- **Comply with law:** respond to legal requests, fulfill regulatory obligations, enforce our Terms of Service

We do not use your personal data to:

- Send marketing emails without your explicit consent
- Sell your information to third parties (we never sell personal data)
- Build advertising profiles
- Train AI/ML models on your private account data without your consent

3.2 Data Flowing Through Our Service

We process data from your connected billing platform exclusively to:

- Run audit checks and generate findings
- Produce audit report PDFs
- Provide ongoing monitoring (for active monthly subscribers)
- Maintain audit history for your reference

We do not:

- Use your billing platform data to train models or improve our detection logic in any way that exposes your specific data to others
- Share your billing platform data with anyone outside our processing infrastructure
- Sell or rent your billing platform data
- Manually browse, search, or analyze your data except as strictly necessary for support, debugging, or legal compliance

3.3 Legal Bases for Processing (GDPR)

If you're in the EU, UK, or another jurisdiction governed by the GDPR or similar law, we rely on the following legal bases:

- **Contract:** processing necessary to provide the service you've signed up for
- **Legitimate interests:** improving the service, preventing fraud, securing our systems
- **Consent:** non-essential cookies, marketing communications (where you opt in)
- **Legal obligation:** complying with law, court orders, regulatory requests

You can object to processing based on legitimate interests at any time by emailing legal@bleedpoint.com.

4. How We Share Data

We share data only as described below. We never sell personal data.

4.1 Subprocessors (Service Providers Helping Us Operate)

We use the following third parties to operate Bleedpoint. Each receives only the data necessary to perform its function and is contractually required to protect it.

Subprocessor	Purpose	Data shared	Location
Amazon Web Services (AWS)	Cloud infrastructure, database, file storage, automated email (SES)	All categories (encrypted at rest)	United States
Stripe	Payment processing for Bleedpoint subscriptions; OAuth platform for connected accounts	Customer billing info; OAuth tokens	United States
Microsoft 365	Inbound email and team mailboxes (kevin@, hello@, support@, etc.)	Email correspondence with our team	United States
Namecheap	Web hosting for the marketing site and DNS services	Visitor IP addresses, HTTP request data, form submissions	United States
CookieYes	Cookie consent management platform	Visitor IP addresses, cookie preferences	European Union
Google Analytics 4	Anonymized usage analytics	Pseudonymous usage data	United States
Microsoft Clarity	Session replay and heatmaps (anonymized)	Pseudonymous interaction data	United States

The current list is also maintained in our Data Processing Agreement (DPA). We will update this list and notify customers of material changes via email or in-app notice.

4.2 Other Sharing Scenarios

We may also share data:

- **With your consent:** when you explicitly authorize us to share with a third party
- **To comply with law:** in response to subpoenas, court orders, or other legitimate legal demands. Where legally permitted, we'll notify you in advance
- **To protect rights and safety:** where we reasonably believe sharing is necessary to prevent fraud, protect our infrastructure, or protect the safety of any person
- **In a business transfer:** if Bleedpoint is acquired, merges, or sells assets, your data may transfer with the business. We'll notify you and you'll have the option to delete your account before any such transfer takes effect.

We never sell personal data, and we never share your billing platform data with third parties for their own commercial purposes.

5. Data Storage and Security

5.1 Where We Store Data

- **Primary storage:** AWS data centers in the United States (us-east-2 region, Ohio)
- **Backups:** AWS-managed backups within the same region, encrypted at rest
- **No EU data residency option (V1):** EU customer data is processed and stored in the US under appropriate transfer mechanisms (see Section 9)

5.2 Security Measures

We protect personal data using:

- **Encryption in transit:** TLS 1.3 for all communication between you and us, and between us and our subprocessors
- **Encryption at rest:** AES-256 encryption for all stored data, with AWS KMS-managed keys
- **OAuth token encryption:** Connected platform OAuth tokens are encrypted with a dedicated KMS key separate from other data
- **Access controls:** Least-privilege IAM roles. Administrative access to our infrastructure is limited and logged via AWS CloudTrail
- **Authentication:** Magic link sign-in for customers (no password storage). Multi-factor authentication required for all administrative access to our infrastructure
- **Network isolation:** Application logic isolated from public internet access where possible. Public endpoints are rate-limited and monitored
- **Audit logging:** All access to customer data is logged with user identifier, timestamp, and action
- **Regular review:** Periodic review of access controls, security configurations, and dependency vulnerabilities

While we use industry-standard practices, no system is perfectly secure. If a breach occurs, we'll notify affected customers within 24 hours of discovering it, per Section 7.

6. Data Retention

We keep different types of data for different lengths of time, balancing your access to the service against minimizing data we hold.

Data type	Retention period
Account record (email, signup info)	Until account deletion + 90-day grace period
Audit metadata (when, what was found)	Indefinite while account is active; 90 days after deletion
Audit reports (PDFs in S3)	Indefinite while account is active; 90 days after deletion

Data type	Retention period
PDF presigned download URLs	7 days from generation (reports remain downloadable from dashboard)
Magic link tokens	15 minutes
Active session tokens (JWTs)	30 days
Stripe OAuth tokens	Active while connected; deleted within 24 hours of disconnect
System logs (CloudTrail, application logs)	90 days hot; archived to AWS Glacier; deleted at 1 year
Database backups (DynamoDB PITR)	35 days
Email correspondence (transactional/support)	1 year, unless related to a transaction or dispute
Email correspondence (billing, refunds, disputes, contracts, legal)	7 years
Billing/transaction records	7 years (US tax/audit requirements)

When you delete your account, the 90-day grace period exists to recover from accidental deletions and to satisfy legal data-retention requirements. After that, account data is permanently deleted from operational systems within 30 days, and from backups as the backup rolling window naturally expires.

You can request earlier deletion under Section 8, subject to legal retention requirements above.

7. Data Breach Notification

If we discover a security incident affecting your personal data:

- We will notify affected customers via email within 24 hours of discovering the incident
- We will provide a description of what happened, what data was affected, and what steps we're taking
- We will report to relevant supervisory authorities where legally required (within 72 hours under GDPR)
- We will document the incident and its resolution, available to affected customers on request

This commitment applies even if we're not strictly required to notify under applicable law.

8. Your Rights

Depending on where you live, you have rights over your personal data. We honor these rights for all customers globally, regardless of jurisdiction, because it's the right thing to do.

8.1 Universal Rights (We Honor for Everyone)

- **Access:** see what personal data we have about you
- **Correction:** fix inaccurate or incomplete data
- **Deletion:** request that we delete your data (subject to legal retention requirements in Section 6)
- **Export:** receive your data in a portable format
- **Opt out of marketing:** stop receiving marketing communications (transactional emails like audit-ready notifications can't be turned off while your account is active)

8.2 Additional Rights for EU/UK Residents (GDPR)

Under the GDPR and UK GDPR, you also have the right to:

- **Object to processing:** where we process based on legitimate interests
- **Restrict processing:** in certain circumstances, ask us to limit how we use your data
- **Withdraw consent:** for processing based on your consent (e.g., non-essential cookies)
- **Lodge a complaint:** with your local data protection authority

The legal basis for processing is described in Section 3.3.

8.3 Additional Rights for California Residents (CCPA/CPRA)

Under the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), you have the right to:

- **Know:** what personal information we collect, use, and share
- **Delete:** request deletion of your personal information
- **Correct:** ask us to correct inaccurate personal information
- **Opt out:** of the sale or sharing of personal information (we do neither, but you have the right regardless)
- **Limit use of sensitive personal information:** restrict our use of any sensitive personal information beyond what's necessary to provide the service
- **Non-discrimination:** we won't discriminate against you for exercising any of these rights

We do not sell or share personal information for cross-context behavioral advertising. We have no "Do Not Sell" mechanism because there's nothing to opt out of.

8.4 How to Exercise Your Rights

Email **legal@bleedpoint.com** with:

- The right you want to exercise
- Enough information to verify your identity (the email associated with your account)

We'll respond within 30 days (or sooner where required by law). For verified requests, exercising your rights is free.

If we deny a request, we'll explain why and inform you of your right to appeal or complain to a supervisory authority.

9. International Data Transfers

If you're located outside the United States and use Bleedpoint, your personal data is transferred to and stored in the United States.

For EU, UK, and Swiss residents, we rely on Standard Contractual Clauses (SCCs) approved by the European Commission as the legal basis for transferring personal data to the US. These clauses are included in our Data Processing Agreement (DPA).

We've conducted reasonable due diligence to confirm that our processing in the US, combined with our security measures, provides adequate protection equivalent to what's required under EU/UK law.

If you have specific questions about cross-border data flows, email legal@bleedpoint.com.

10. Children's Data

Bleedpoint is intended for use by businesses, not individuals under 18. We do not knowingly collect personal data from children under 18. If you believe we have collected data from a child, contact legal@bleedpoint.com and we'll delete it promptly.

11. Changes to This Policy

We may update this Privacy Policy from time to time. When we do:

- **Minor changes (typos, clarifications):** we'll update the document and effective date without separate notice
- **Material changes (new data uses, new subprocessors, narrowed rights):** we'll notify you via email at least 30 days before they take effect

The "Effective Date" at the top of this policy reflects the most recent update. Past versions are available on request.

12. Contact Us

For privacy questions, requests, or concerns:

- General: hello@bleedpoint.com
- Privacy and legal: legal@bleedpoint.com
- Security disclosures: security@bleedpoint.com

You can also write to us:

CloudSec Global LLC Attn: Bleedpoint Privacy 6881 W Charleston Blvd, Ste A, Unit #5209 Las Vegas, NV 89117 United States

Bleedpoint is a product of **CloudSec Global LLC**, a Nevada limited liability company.

This Privacy Policy is effective as of April 26, 2026.