Data Processing Agreement (DPA)

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 Data Processing Agreement ("DPA") is entered into between you (the "Customer," acting as Data Controller) and CloudSec Global LLC, operating the Bleedpoint service (the "Processor"). It governs the processing of personal data carried out by Bleedpoint on your behalf in connection with the Bleedpoint Revenue Audit Service.

This DPA forms part of, and is incorporated into, the Bleedpoint Terms of Service. In the event of a conflict between this DPA and the Terms of Service, this DPA controls with respect to the processing of personal data.

This DPA is designed to comply with:

- The EU General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR")
- The UK General Data Protection Regulation and the Data Protection Act 2018 ("UK GDPR")
- The California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act ("CCPA/CPRA")
- Other applicable data protection laws

1.1 Definitions

For the purposes of this DPA, the following definitions apply:

- **"Applicable Data Protection Laws":** all laws and regulations applicable to the processing of Personal Data under this DPA, including GDPR, UK GDPR, CCPA/CPRA, and equivalent laws in other jurisdictions.
- **"Customer Data":** all data, including Personal Data, that Customer or its end users transmit to Bleedpoint, or that Bleedpoint accesses on Customer's behalf via authorized integrations (such as Stripe Connect).
- **"Data Controller" (or "Controller"):** the entity that determines the purposes and means of processing Personal Data. For the purposes of Customer Data, this is the Customer.
- **"Data Processor" (or "Processor"):** the entity that processes Personal Data on behalf of the Controller. For the purposes of this DPA, this is Bleedpoint.
- **"Data Subject":** an identified or identifiable natural person to whom Personal Data relates.
- **"Personal Data":** any information relating to an identified or identifiable natural person, as defined in Applicable Data Protection Laws.

- **"Processing":** any operation performed on Personal Data, including collection, recording, storage, use, disclosure, deletion, or destruction.
- **"Sub-processor":** any third party engaged by Bleedpoint to process Personal Data on behalf of Customer.
- **"Standard Contractual Clauses" (or "SCCs"):** the standard contractual clauses approved by the European Commission for the transfer of Personal Data from the EEA to third countries, as updated from time to time.
- **"Security Incident":** any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

2. Roles of the Parties

2.1 Controller and Processor Relationship

For Personal Data flowing through the Bleedpoint service:

- **Customer is the Data Controller.** Customer determines the purposes and means of processing Personal Data of Customer's own customers (whose data flows from Customer's connected billing platform into Bleedpoint).
- **Bleedpoint is the Data Processor.** Bleedpoint processes Personal Data on Customer's behalf, in accordance with Customer's documented instructions, to provide the Bleedpoint service.

2.2 Bleedpoint as Independent Controller

For limited categories of Personal Data, Bleedpoint acts as an independent Controller:

- **Customer's account information** (Customer's own email, billing details, account preferences) — Bleedpoint collects this directly from Customer to provide the service.
- **Aggregated and anonymized analytics** — where data is anonymized so that individuals can no longer be identified.
- **Operational data required by law or for security** (audit logs, fraud prevention).

For this category, Bleedpoint's processing is governed by the Bleedpoint Privacy Policy, not this DPA.

2.3 CCPA Service Provider Status

For Customer Data subject to CCPA/CPRA, Bleedpoint acts as a "Service Provider" within the meaning of the CCPA/CPRA. Bleedpoint will not:

- Sell or share Customer Data
- Retain, use, or disclose Customer Data for any purpose other than performing the services specified in the Terms of Service
- Combine Customer Data with personal information from other sources, except as permitted under CCPA/CPRA Section 1798.140(ag)(1)

3. Subject Matter and Details of Processing

3.1 Subject Matter

Bleedpoint processes Customer Data to provide automated revenue audit services, including identifying potential revenue leakage in Customer's connected billing platform.

3.2 Duration of Processing

Bleedpoint processes Customer Data for the duration of Customer's active subscription, plus any retention period specified in Section 9 of this DPA and the Bleedpoint Privacy Policy.

3.3 Nature and Purpose of Processing

Processing operations include:

- Receiving Customer Data via authorized OAuth integration with the connected billing platform
- Storing Customer Data in encrypted form in Bleedpoint's infrastructure
- Analyzing Customer Data to detect revenue leakage patterns
- Generating audit reports based on the analysis
- Delivering reports to Customer
- Maintaining audit history while Customer's account is active

3.4 Categories of Data Subjects

Customer Data may relate to the following categories of Data Subjects:

- Customer's own customers (the people who are billed through Customer's billing platform)
- Customer's end users
- Other natural persons whose information is contained in Customer's connected billing platform records

3.5 Categories of Personal Data

The Personal Data processed by Bleedpoint may include:

- Email addresses
- Names (where present in the connected billing platform)
- Customer identifiers and account creation timestamps
- Subscription and billing history (statuses, plans, amounts, dates)
- Payment records (success/failure, amounts, retry attempts) — excluding card numbers and payment credentials
- Invoice metadata (amounts, dates, payment status)
- Coupon and discount usage records

Bleedpoint does not process the following categories of data:

- Credit card numbers, bank account numbers, or any payment credentials
- Tax identification numbers (SSN, EIN, VAT IDs of Data Subjects)
- Authentication credentials of any kind
- Special categories of Personal Data under Article 9 GDPR (health, biometric, political, religious data, etc.) unless Customer specifically configures the processing of such data, which Bleedpoint does not request or require
- Children's data — Customer represents that the connected billing platform does not contain Personal Data of children under 16 (or applicable local age threshold for digital consent)

4. Customer's Obligations as Data Controller

4.1 Lawful Basis

Customer warrants and represents that:

- Customer has a valid legal basis under Applicable Data Protection Laws to process Customer Data and to authorize Bleedpoint to process Customer Data on its behalf
- Customer has provided all required notices to Data Subjects regarding the processing
- Customer has obtained any necessary consents from Data Subjects, where required by Applicable Data Protection Laws

4.2 Customer Instructions

Customer's instructions for processing Personal Data are documented in:

- This DPA
- The Terms of Service
- The Bleedpoint Privacy Policy
- Customer's configuration choices within the Bleedpoint application

Bleedpoint will only process Customer Data in accordance with these documented instructions, except where required by Applicable Data Protection Laws or other legal obligations to which Bleedpoint is subject.

4.3 Notification of Unlawful Instructions

If Bleedpoint believes that an instruction from Customer would violate Applicable Data Protection Laws, Bleedpoint will notify Customer of this concern. Customer remains responsible for the lawfulness of its instructions.

5. Bleedpoint's Obligations as Data Processor

5.1 Compliance with Customer Instructions

Bleedpoint will process Personal Data only:

- On documented instructions from Customer (as set out in Section 4.2)
- As necessary to provide the service under the Terms of Service
- As required by Applicable Data Protection Laws (in which case Bleedpoint will inform Customer of the legal requirement before processing, unless prohibited by law)

5.2 Confidentiality

Bleedpoint will ensure that all personnel authorized to process Personal Data:

- Are bound by appropriate confidentiality obligations
- Receive appropriate training on data protection requirements
- Process Personal Data only as necessary for their assigned roles

5.3 Security Measures

Bleedpoint will implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing, as described in Section 7 of this DPA.

5.4 Assistance to Customer

Bleedpoint will assist Customer, taking into account the nature of processing and the information available, in fulfilling Customer's obligations under Applicable Data Protection Laws, including:

- Responding to Data Subject requests (Section 8)
- Conducting Data Protection Impact Assessments (DPIAs)
- Consulting with supervisory authorities, where required
- Notifying Data Subjects of Security Incidents, where required

6. Sub-processors

6.1 General Authorization

Customer provides general authorization for Bleedpoint to engage Sub-processors as listed in Section 6.2.

6.2 Current Sub-processors

As of the Effective Date, Bleedpoint engages the following Sub-processors:

Sub-processor	Purpose	Location	Transfer Mechanism (for non-US Customers)
Amazon Web Services, Inc.	Cloud infrastructure, database, file storage, automated email (SES)	United States	SCCs included in AWS DPA
Stripe, Inc.	Payment processing for Bleedpoint subscriptions; OAuth platform for connected accounts	United States	SCCs included in Stripe DPA
Microsoft Corporation (Microsoft 365)	Inbound email and team mailboxes	United States	SCCs / Microsoft EU Data Boundary
Namecheap, Inc.	Web hosting for marketing site and DNS services	United States	SCCs as published by Namecheap
CookieYes Limited	Cookie consent management platform	European Union	Direct EU establishment; UK adequacy decision
Google LLC (Google Analytics 4)	Anonymized usage analytics	United States	SCCs / EU-US Data Privacy Framework
Microsoft Corporation (Microsoft Clarity)	Session replay and heatmaps (anonymized)	United States	SCCs / EU-US Data Privacy Framework

6.3 Sub-processor Obligations

Before engaging any Sub-processor, Bleedpoint will enter into a written agreement that:

- Imposes data protection obligations no less protective than those in this DPA
- Requires the Sub-processor to process Personal Data only as instructed by Bleedpoint and for the purposes Bleedpoint has authorized
- Ensures appropriate security measures equivalent to those described in Section 7
- Includes audit and inspection rights

Bleedpoint remains liable to Customer for any acts or omissions of its Sub-processors that result in a breach of this DPA.

6.4 Notification of New or Replacement Sub-processors

Bleedpoint will notify Customer at least 30 days in advance of adding or replacing any Sub-processor, by:

- Email to Customer's account email address, or
- In-app notice within the Bleedpoint application, or
- Updating the Sub-processor list at bleedpoint.com/dpa with notice of the update

6.5 Customer Right to Object

Customer may object to a new or replacement Sub-processor on reasonable grounds related to data protection within 30 days of notification. If Customer reasonably objects, Bleedpoint will:

- Use commercially reasonable efforts to make the service available without the objected-to Sub-processor, or
- Allow Customer to terminate the affected service with a pro-rated refund of any prepaid fees

If Customer does not object within 30 days, the new Sub-processor is deemed accepted.

7. Security of Processing

7.1 Security Measures

Bleedpoint implements the following technical and organizational measures, taking into account the state of the art, costs of implementation, and the nature, scope, context, and purposes of processing:

Encryption:

- All Personal Data encrypted in transit using TLS 1.3 or higher
- All Personal Data encrypted at rest using AES-256 with AWS KMS-managed keys
- OAuth tokens for connected billing platforms encrypted with a dedicated KMS key

Access Controls:

- Least-privilege IAM roles for all infrastructure access
- Multi-factor authentication required for all administrative access
- Role-based access controls within the application
- Audit logging of all access to Customer Data via AWS CloudTrail

Authentication:

- Magic link authentication for Customer access (no password storage)
- Session tokens (JWTs) signed with secrets stored in AWS Secrets Manager
- Token rotation on each authentication event

Network Security:

- Application logic isolated from public internet where possible
- Public endpoints rate-limited and monitored for abuse
- Web Application Firewall (WAF) protection for public endpoints

Data Integrity and Availability:

- Database backups with point-in-time recovery (35 days)
- CloudTrail logging of all infrastructure changes

- S3 versioning for critical buckets
- Disaster recovery procedures documented and tested

Personnel Security:

- Background checks for personnel with access to Personal Data, where legally permitted
- Mandatory data protection and security training
- Confidentiality agreements signed by all personnel
- Access revocation upon role change or termination

Incident Response:

- Documented incident response plan
- Continuous monitoring of infrastructure for security events
- 24-hour notification commitment to Customer following discovery of a Security Incident (Section 10)

7.2 Updates to Security Measures

Bleedpoint may update its security measures from time to time, provided that updates do not materially decrease the level of protection. Material changes will be communicated to Customer in advance.

8. Data Subject Rights

8.1 Bleedpoint's Assistance

To the extent legally required, Bleedpoint will assist Customer in fulfilling Data Subject requests by:

- Providing tools within the Bleedpoint application to access, export, correct, or delete Personal Data
- Responding to Customer's request for assistance with Data Subject requests within a reasonable timeframe
- Implementing technical measures to support Data Subject rights

8.2 Direct Requests to Bleedpoint

If Bleedpoint receives a Data Subject request directly (rather than through Customer), Bleedpoint will:

- Inform the Data Subject that the request must be directed to Customer
- Forward the request to Customer where possible and lawful
- Not respond to the request directly unless legally required to do so

8.3 Data Subject Categories

Customer acknowledges that Data Subjects under this DPA primarily include Customer's own customers and end users — individuals whose Personal Data flows through Customer's connected billing platform into Bleedpoint. Customer is responsible for managing direct relationships with these Data Subjects.

9. Data Retention and Deletion

9.1 Retention During Service Term

Bleedpoint retains Personal Data for the periods specified in the Bleedpoint Privacy Policy and as necessary to provide the service.

9.2 Deletion Upon Termination

Upon termination of Customer's subscription:

- Audit metadata, audit reports, and account data are retained for a 90-day grace period to allow for accidental termination recovery
- After the grace period, Personal Data is permanently deleted from operational systems within 30 days
- Personal Data in backups is deleted as the backup rolling window naturally expires (within 35 days of operational deletion)

9.3 Customer-Initiated Deletion

Customer may request deletion of specific Personal Data at any time by:

- Using deletion features within the Bleedpoint application (where available)
- Emailing legal@bleedpoint.com with a written request

Bleedpoint will complete the requested deletion within 30 days of receiving a verifiable request, except where retention is required by Applicable Data Protection Laws.

9.4 Legally Required Retention

Bleedpoint may retain Personal Data after termination only to the extent required by Applicable Data Protection Laws (e.g., billing records for tax compliance, audit logs for security investigations). Where this applies, Bleedpoint will:

- Limit further processing to the legally required purposes
- Continue to apply security measures described in Section 7
- Delete the Personal Data when retention is no longer legally required

10. Security Incident Notification

10.1 Notification Timeline

If Bleedpoint becomes aware of a Security Incident affecting Personal Data, Bleedpoint will notify Customer without undue delay, and in any event within 24 hours of becoming aware of the incident.

10.2 Information Provided

The notification will include, to the extent known at the time:

- A description of the nature of the Security Incident
- The categories and approximate number of Data Subjects affected
- The categories and approximate volume of Personal Data records affected
- The likely consequences of the Security Incident
- Measures taken or proposed to address the Security Incident and mitigate its effects
- Contact details for further information

If full information is not available at the time of initial notification, Bleedpoint will provide updates as information becomes available.

10.3 Customer's Notification Obligations

Customer is responsible for notifying:

- Affected Data Subjects, where required by Applicable Data Protection Laws
- Supervisory authorities, where required by Applicable Data Protection Laws (e.g., within 72 hours under GDPR Article 33)

Bleedpoint will provide reasonable assistance to Customer in fulfilling these obligations.

10.4 No Admission of Liability

Notification of a Security Incident is not, and will not be construed as, an admission by Bleedpoint of fault or liability with respect to the incident.

11. Audits and Inspections

11.1 Audit Rights

Customer has the right to verify Bleedpoint's compliance with this DPA. Bleedpoint will make available to Customer, upon reasonable written request:

- Information necessary to demonstrate compliance with this DPA
- Results of relevant third-party audits or certifications (where Bleedpoint has obtained them)
- Responses to specific compliance questions

11.2 Remote Audits

For Customers that require additional audit verification to comply with their own obligations under Applicable Data Protection Laws, audits will be conducted remotely. Specifically:

- Audits must be requested in writing with at least 30 days' notice
- Audits are limited to once per 12-month period (except in case of a Security Incident)

- Audits are conducted via documented evidence review, video conference, and screen-share sessions during business hours, in a manner that does not unreasonably interfere with Bleedpoint's operations
- No physical or on-site inspection of Bleedpoint's facilities is required or permitted; Bleedpoint operates as a cloud-native service with no physical office or data center to inspect
- Inspections of Sub-processor data centers are subject to those Sub-processors' own audit policies (Section 11.3)
- The Customer bears its own audit costs, including any third-party auditor fees; Bleedpoint bears the cost of providing reasonable cooperation
- The auditor must sign appropriate confidentiality agreements
- Bleedpoint may require the use of a mutually acceptable third-party auditor

11.3 Sub-processor Audits

For Sub-processors, Bleedpoint will use commercially reasonable efforts to obtain audit reports or to facilitate Customer's audit rights, subject to the Sub-processor's own audit policies.

12. International Data Transfers

12.1 Cross-Border Transfers

Bleedpoint processes Personal Data primarily in the United States. Where Customer Data is transferred from the European Economic Area (EEA), United Kingdom, or Switzerland to the United States or other third countries, Bleedpoint relies on the legal mechanisms described below.

12.2 Standard Contractual Clauses (SCCs)

Where required by Applicable Data Protection Laws, the parties agree to be bound by the European Commission's Standard Contractual Clauses (Module 2: Controller to Processor) for transfers from the EEA to the United States, as published in Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as amended.

The SCCs are incorporated into this DPA by reference. The following details apply:

- **Module:** Module 2 (Controller to Processor)
- **Clause 7 (Docking Clause):** applies
- **Clause 9 (Sub-processors):** Option 2 (general written authorization), with 30 days' notice as set out in Section 6.4
- **Clause 11 (Redress):** the optional independent dispute resolution provision does not apply
- **Clause 17 (Governing Law):** the law of Ireland
- **Clause 18 (Choice of Forum and Jurisdiction):** the courts of Ireland

12.3 UK International Data Transfer Addendum

For transfers subject to UK GDPR, the parties incorporate the UK International Data Transfer Addendum (IDTA) issued by the UK Information Commissioner's Office, version published 21 March 2022, as a supplement to the SCCs above. The IDTA tables are completed as follows:

- Table 1 (Parties): Customer and Bleedpoint as identified in the Terms of Service
- Table 2 (Selected Modules): Module 2 SCCs as described in Section 12.2
- Table 3 (Appendix Information): as described in this DPA
- Table 4 (Ending the Addendum): either party may end the Addendum where its content changes, as set out in Section 19 of the IDTA

12.4 Swiss Data Transfers

For transfers from Switzerland, the parties agree that the SCCs will be interpreted to apply to such transfers, with the following modifications:

- References to GDPR will be interpreted as references to the Swiss Federal Act on Data Protection (FADP)
- References to "EU member state" will include Switzerland
- The competent supervisory authority is the Federal Data Protection and Information Commissioner of Switzerland

12.5 Supplementary Measures

In light of the Schrems II ruling and similar legal developments, Bleedpoint has implemented supplementary measures to protect Personal Data transferred to the United States, including:

- Encryption at rest with keys managed within the controller's jurisdiction where feasible
- Resistance to government access requests through legal challenge where lawful
- Transparency reports on government data requests, where legally permitted
- Contractual protections from Sub-processors regarding government access requests

13. Liability

13.1 Limitation of Liability

The liability of each party under this DPA is subject to the limitations of liability set out in the Terms of Service, except where Applicable Data Protection Laws prohibit such limitation.

13.2 GDPR Liability Regime

With respect to claims by Data Subjects under GDPR Article 82:

- Each party is responsible for its own compliance with GDPR
- The parties' allocation of liability follows GDPR Article 82(4) and (5)

- Nothing in this DPA limits a Data Subject's right to claim compensation directly from either party

14. General Provisions

14.1 Term and Termination

This DPA remains in effect for as long as Bleedpoint processes Personal Data on behalf of Customer. Upon termination of the Terms of Service, this DPA terminates, except for provisions that by their nature should survive (including data retention obligations in Section 9 and confidentiality obligations).

14.2 Modifications

Bleedpoint may update this DPA from time to time:

- For minor changes (clarifications, corrections, Sub-processor list updates per Section 6.4), Bleedpoint will update the document and effective date
- For material changes (changes to scope of processing, new processing purposes, weakening of obligations), Bleedpoint will provide at least 30 days' notice to Customer

14.3 Severability

If any provision of this DPA is held to be invalid or unenforceable, the rest of the DPA remains in effect, and the invalid provision is reinterpreted to come as close as possible to its original intent while remaining enforceable.

14.4 Order of Precedence

In the event of conflict between documents, the order of precedence is:

1. The Standard Contractual Clauses (where applicable)
2. This DPA
3. The Terms of Service
4. The Privacy Policy

14.5 Governing Law

This DPA is governed by the laws of the State of Nevada, United States, except that the SCCs are governed by the law identified in Section 12.2.

14.6 Entire Agreement

This DPA, together with the Terms of Service, the Privacy Policy, and (where applicable) the SCCs, constitutes the entire agreement between the parties regarding the processing of Personal Data.

15. Contact Information

For questions about this DPA or to exercise rights under it:

- Data Protection inquiries: legal@bleedpoint.com
- Security disclosures: security@bleedpoint.com
- General questions: hello@bleedpoint.com

You can also write to us:

CloudSec Global LLC Attn: Bleedpoint Data Protection 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 DPA is effective as of April 26, 2026, and applies to all Personal Data processed by Bleedpoint on Customer's behalf from that date forward.

By using the Bleedpoint service, Customer accepts this DPA and authorizes Bleedpoint to process Personal Data in accordance with its terms.