

ConsentBit Data Processing Agreement

Version 1.0 | Effective date: 24 October 2026.

This Data Processing Agreement ("**DPA**") forms part of the ConsentBit Terms of Service (the "**Agreement**") between:

- **Seattle New Media, LLC**, a Florida limited liability company doing business as ConsentBit, 5608 17th Ave. NW, Suite 581, Seattle, WA 98107, USA ("**ConsentBit**", "**we**", "**Processor**"); and
- The customer that has accepted the Agreement ("**Customer**", "**you**", "**Controller**").

It applies whenever ConsentBit processes Personal Data on the Customer's behalf through the ConsentBit service, for every website in the Customer's account, including websites added later. By accepting the Agreement, the Customer accepts the current version of this DPA. Where this DPA and the Agreement conflict about Personal Data, this DPA wins. Where this DPA and the SCCs conflict, the SCCs win.

1. Definitions

1.1 Data Protection Laws: all privacy laws that apply to the processing, including the EU GDPR (Regulation 2016/679), the UK GDPR and Data Protection Act 2018, the Swiss Federal Act on Data Protection ("**FADP**"), the California Consumer Privacy Act as amended by the CCPA ("**CCPA**") and other US state privacy laws, Brazil's LGPD, Quebec's Law 25, Canada's PIPEDA, and any other law that applies to the Customer's website.

1.2 Personal Data: any information about an identified or identifiable person that ConsentBit processes for the Customer under the Agreement.

1.3 Visitor: a person who visits a website on which the Customer has installed the ConsentBit banner.

1.4 Consent Record: the record ConsentBit stores each time a Visitor makes a choice on the banner.

1.5 Sub-processor: a third party that ConsentBit uses to process Personal Data for the Customer.

1.6 Security Incident: a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.

1.7 SCCs: the Standard Contractual Clauses approved by Commission Implementing Decision (EU) 2021/914.

1.8 "Controller", "Processor", "Data Subject", "Processing", "Personal Data Breach" and "Supervisory Authority" have the meanings given in the GDPR. "Business", "Service Provider", "Sell" and "Share" have the meanings given in the CCPA.

2. Roles and scope

2.1 For Personal Data about Visitors, the Customer is the Controller (under the CCPA, the "Business") and ConsentBit is the Processor (under the CCPA, the "Service Provider").

2.2 If the Customer is itself a processor for another controller (for example, an agency installing the banner on a client's website), ConsentBit is the Customer's sub-processor, the Customer confirms that it has its controller's authorisation to use ConsentBit, and the Customer's instructions under this DPA are given on behalf of that controller.

2.3 For data about the Customer's own account (account users' names, emails, billing), ConsentBit is an independent Controller. That data is covered by the ConsentBit Privacy Policy, not this DPA.

2.4 Details of the processing are in Annex I.

2.5 The Consent ID is random, is stored in a first-party cookie on each website separately, and is not linked across websites or to a Visitor's identity. ConsentBit will not use Personal Data to track Visitors across different Customer websites except as expressly documented in this DPA.

3. The Customer's responsibilities

The Customer:

- 3.1 Decides which cookies and scripts to use and puts each in the correct category in the banner settings;
- 3.2 Publishes and maintains a privacy policy on its website, linked from the banner;
- 3.3 Has a lawful basis for the processing and gives Visitors the information Data Protection Laws require;
- 3.4 Answers Visitors' requests, using the tools ConsentBit provides (section 8);
- 3.5 Gives instructions that comply with Data Protection Laws; and
- 3.6 Keeps its account login details secure and limits dashboard access to people who need it.

4. ConsentBit's obligations

ConsentBit will:

- 4.1 **Instructions.** Process Personal Data only on the Customer's documented instructions, including for transfers outside the EEA, UK and Switzerland, unless the law requires otherwise, in which case we will tell the Customer first unless the law forbids it. The Agreement, this DPA and the Customer's settings in the ConsentBit dashboard are the Customer's complete instructions. Instructions given orally must be confirmed in writing or by email. We will tell the Customer promptly if we believe an instruction breaks Data Protection Laws.
- 4.2 **Confidentiality.** Make sure everyone authorised to process Personal Data is bound by confidentiality.
- 4.3 **Security.** Apply the technical and organisational measures in Annex II.
- 4.4 **Sub-processors.** Follow section 6.
- 4.5 **Assistance.** Help the Customer respond to Visitor requests (section 8), and with security, breach notification, data protection impact assessments and prior consultation with a Supervisory Authority, taking into account the nature of the processing and the information available to us.
- 4.6 **Deletion and return.** Return or delete Personal Data as set out in section 10.
- 4.7 **Audits.** Make available the information needed to show compliance with this DPA, and allow audits (section 11).
- 4.8 **Authorities.** Tell the Customer without undue delay if a Supervisory Authority inspects, investigates or contacts ConsentBit about Personal Data processed for the Customer, unless the law forbids it.
- 4.9 **Government requests.** If a public authority asks ConsentBit for access to Personal Data processed for the Customer, we will: tell the Customer (unless the law forbids it); disclose only what is legally required after reviewing the request's lawfulness; challenge requests we consider unlawful where there are reasonable grounds; and keep a record of such requests. ConsentBit has received no such request to date.
- 4.10 **Self-checks.** ConsentBit will review the technical and organisational measures in Annex II at least once a year and update them as technology and risks change.

5. US state privacy laws (CCPA and similar)

When acting as a Service Provider or Processor under the CCPA or another US state privacy law, ConsentBit:

5.1 Processes Personal Data only for the limited and specified business purpose of providing the consent-management service described in Annex I;

5.2 Will not Sell or Share Personal Data;

5.3 Will not retain, use or disclose Personal Data outside the direct business relationship with the Customer, or for any purpose other than the business purpose, including any commercial purpose;

5.4 Will not combine Personal Data with personal information it receives from other sources or collects from its own interactions with a consumer, except as the CCPA permits;

5.5 Will comply with the CCPA, give the same level of privacy protection the CCPA requires, and notify the Customer if it can no longer meet its obligations;

5.6 Allows the Customer to take reasonable and appropriate steps to stop and remedy unauthorised use of Personal Data; and

5.7 Certifies that it understands and will comply with these restrictions.

6. Sub-processors

6.1 The Customer gives general written authorisation for ConsentBit to use Sub-processors. The current list is in Annex III of this DPA, published at <https://www.consentbit.com/dpa>.

6.2 We will give at least 30 days' notice before adding or replacing a Sub-processor, by updating Annex III and emailing the Customer's account email.

6.3 The Customer may object on reasonable data-protection grounds by email to privacy@consentbit.com within that 30-day period. If it does:

- (a) we will discuss the objection with the Customer in good faith and, where possible, offer a reasonable alternative (such as not using the new Sub-processor for the Customer's data);
- (b) if we cannot resolve the objection within 30 days of receiving it, the Customer may terminate the affected part of the service by written notice, without penalty; and
- (c) ConsentBit will refund prepaid fees for the unused period of the terminated service.

6.4 We impose data-protection obligations on each Sub-processor that are at least as protective as this DPA, and remain responsible to the Customer for each Sub-processor's performance.

7. International transfers

7.1 ConsentBit is based in the United States. Consent Records are stored in the European Union, in a Cloudflare D1 database with EU jurisdiction (Annex III). Personal Data may still pass through other countries when Cloudflare's global network serves the banner, and ConsentBit staff may access it from the United States for support and maintenance. ConsentBit is **not** certified under the EU-US Data Privacy Framework; transfers rely on the SCCs below.

7.2 **EU Standard Contractual Clauses.** For transfers of Personal Data from the EEA to a country without an adequacy decision, the parties agree to the SCCs, which are incorporated into this DPA by reference, as follows:

- (a) Module Two (Controller to Processor) applies where the Customer is a controller; Module Three (Processor to Processor) applies where the Customer is a processor (section 2.2);

- (b) Clause 7 (docking clause) applies;
- (c) Clause 9(a): Option 2 (general written authorisation), with the notice period in section 6.2;
- (d) Clause 11(a): the optional language does not apply;
- (e) Clause 13: (i) where the Customer is established in an EU Member State, the supervisory authority of that Member State; (ii) where the Customer is not established in the EU but falls under Article 3(2) GDPR and has appointed an EU representative, the supervisory authority of the Member State where the representative is established; (iii) where the Customer is not established in the EU and has no representative, the supervisory authority of the Member State where the Visitors whose data is transferred are located, as set out in Clause 13(a) of the SCCs;
- (f) Clause 17: Option 1, the law of Ireland;
- (g) Clause 18: the courts of Ireland;
- (h) Annexes I.A, I.B and I.C of the SCCs are completed by Annex I of this DPA; Annex II by Annex II; Annex III by Annex III.

7.3 Customer acts as processor. Where Module Three applies, the Customer will pass on to its controller any information ConsentBit provides under the SCCs, and ConsentBit may rely on the Customer's instructions as the controller's instructions.

7.4 UK. For transfers from the UK, the SCCs apply as amended by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B1.0) issued by the Information Commissioner. Tables 1 to 3 of the Addendum are completed by sections 7.2 and Annexes I–III of this DPA. Table 4: either party may end the Addendum as set out in its Section 19.

7.5 Switzerland. For transfers from Switzerland, the SCCs apply with these changes: references to the GDPR are read as references to the FADP where the FADP applies; the Federal Data Protection and Information Commissioner is the competent supervisory authority for those transfers; the term "Member State" includes Switzerland, so Swiss data subjects can enforce their rights in Switzerland.

7.6 ConsentBit will document the transfer impact assessment and supplementary measures applicable to its verified data flows before making this DPA effective, and will provide an appropriate summary to the Customer on request.

7.7 If the SCCs and this DPA conflict, the SCCs win.

8. Visitor requests

8.1 If a Visitor contacts ConsentBit directly about Personal Data we process for a Customer, we will forward the request to the Customer within 2 working days and will not answer it ourselves, unless the Customer asks us to.

8.2 ConsentBit provides the Customer with tools in the ConsentBit dashboard to respond to Visitor requests, including the capabilities listed below to the extent supported by the service.

- (a) find a Visitor's records by the Consent ID, which the Visitor can read in their own browser storage under the cookie named "consentbit-consentid";
- (b) export those records as a file (access and portability requests); and
- (c) delete those records (erasure requests).

8.3 If the Customer cannot answer a request with these tools, we will help on request, at no extra cost unless requests are manifestly unfounded or excessive.

9. Security Incidents

9.1 ConsentBit will notify the Customer without undue delay, and in any case within 48 hours, after becoming aware of a Security Incident affecting the Customer's Personal Data. Notice goes to the Customer's account email.

9.2 The notice will describe, as far as known: the nature of the incident; the categories and approximate number of Visitors and records affected; a contact point at ConsentBit; the likely consequences; and the measures taken or proposed. Information may be given in stages.

9.3 We will take reasonable steps to contain the incident and limit its effects, keep a record of every Security Incident, and help the Customer meet its own notification duties to Supervisory Authorities and Visitors.

9.4 Notifying a Security Incident is not an admission of fault or liability.

10. Retention, return and deletion

10.1 **During the Agreement.** Consent Records are deleted according to the shortest technically practicable and legally justified retention schedule approved for the relevant record type and plan: Free plan: shown in the dashboard for 3 months and kept for 12 months; paid plans: 12 months; records of US Visitors' choices (including opt-outs) under the CCPA: 24 months on every plan. ConsentBit will document the applicable periods and allow deletion requests as described in section 8, subject to lawful retention obligations.

10.2 **When the Agreement ends, or the Customer removes a website.** The Customer may export its Consent Records before the end date. ConsentBit deletes the Consent Records for that website within 30 days, unless the law requires us to keep them.

10.3 **Backups.** Deleted Personal Data is removed from active systems and backups according to the verified deletion and recovery schedules: from active systems at once, and from backups within 30 days (the Cloudflare D1 recovery window).

10.4 **Proof of deletion.** On request, ConsentBit will confirm in writing what was deleted and when.

11. Audits

11.1 On request, ConsentBit will give the Customer the information reasonably needed to show compliance with this DPA, including a description of our security measures, results of the reviews described in section 4.10, to the extent disclosable, and the Sub-processor's current certifications (such as Cloudflare's SOC 2 report and ISO 27001 certificate, where Cloudflare allows them to be shared).

11.2 If that information is not enough, or a Supervisory Authority requires it, the Customer (or an independent auditor bound by confidentiality and not a competitor of ConsentBit) may carry out an audit at most once a year, with at least 30 days' notice, during business hours, at the Customer's cost. Audits after a Security Incident, or required by a Supervisory Authority, are not limited to once a year.

12. Liability

Each party's liability under this DPA is subject to the limits and exclusions, including any approved aggregate liability cap, in the Agreement, except where Data Protection Laws or the SCCs do not allow those limits. Nothing in this DPA limits a Visitor's rights under Article 82 GDPR.

13. Term and changes

13.1 This DPA lasts as long as ConsentBit processes Personal Data for the Customer. Sections that by their nature should survive (including sections 9, 10 and 12) survive termination.

13.2 ConsentBit may update this DPA to reflect changes in law or in the service. We will email the Customer at least 30 days before a change that reduces the Customer's protection takes effect. Each version is dated and numbered.

13.3 The Customer may request an executed PDF of this same master DPA by email to privacy@consentbit.com. Any signature page and customer-specific information shall be generated from the then-approved version of this DPA, without creating or maintaining a separately edited agreement.

14. Governing law

This DPA is governed by the law that governs the Agreement, except where the SCCs or Data Protection Laws require otherwise.

Annex I: Description of the processing

A. List of parties

Data exporter (Controller, or Processor under section 2.2)

- Name, address, contact person: as identified in the Customer's ConsentBit account at acceptance.
- Activities: operating the website(s) on which the ConsentBit banner is installed.
- Role: Controller (Module Two) or Processor (Module Three).
- Signature and date: acceptance of the Agreement when the Customer's ConsentBit account was created; a customer-specific execution page is provided only upon request.

Data importer (Processor)

- Name: Seattle New Media, LLC, doing business as ConsentBit.
- Address: 5608 17th Ave. NW, Suite 581, Seattle, WA 98107, USA.
- Contact for data protection: privacy@consentbit.com.
- Activities: providing a cookie-consent management service.
- Role: Processor.

B. Description of the transfer

Data subjects	Visitors to the Customer's website(s).
Sensitive data	None. The service is not designed to collect special categories of data.
Frequency	Continuous, each time a Visitor makes or changes a choice.
Nature of processing	Collecting, storing, retrieving, exporting and deleting Consent Records; displaying them to the Customer; serving the banner script.
Purpose	To record and prove Visitors' consent choices, apply those choices on the Customer's website (blocking or allowing cookies and scripts), and help the Customer answer Visitor requests.

Retention	Record-specific periods and deletion terms as approved and recorded in section 10.1; Free plan: shown in the dashboard for 3 months and kept for 12 months; paid plans: 12 months; records of US Visitors' choices (including opt-outs) under the CCPA: 24 months on every plan; website-removal and account-termination deletion as described in sections 10.2–10.4.
Transfers to Sub-processors	As in Annex III, for the same purpose and duration.

Categories of Personal Data, and why each is needed

Data item	Why it is needed
Consent ID (random, stored in the Visitor's browser)	Lets the Visitor and the Customer find the record later, as proof of consent or to answer a request.
Shortened IP address (IPv4 to /24, IPv6 to /48; the full address is never stored)	Proof that the choice came from a real request; rough location when no country header is available.
Country and region	Decides which law and which banner apply (for example GDPR, CCPA, Law 25).
Browser user agent	Tells real visits apart from bots and automated traffic; shows the device type in proof records.
Page domain	Shows on which website consent was given.
Date and time of the choice; expiry	Shows when consent was given and when it must be asked again.
Choice per category (necessary, analytics, marketing, preferences)	The consent itself.
Method (banner, preference panel, Global Privacy Control signal)	Shows how the choice was made, needed to prove a valid opt-out under US laws.
Law that applied	Shows which rules the banner followed for this Visitor.
Fingerprint of the banner text and privacy-policy link shown	Proves what information the Visitor saw when choosing.
IAB TCF purpose and vendor choices (TCF banners only)	Required by the IAB Transparency & Consent Framework to pass the choice to ad vendors.

Not collected: names, email addresses, account identifiers, or any other direct identifier of Visitors.

C. Competent supervisory authority

Determined under section 7.2(e) (Clause 13 of the SCCs).

Annex II: Technical and organisational measures

Organised under Article 32 GDPR.

1. Confidentiality

- Access control (dashboard): login by email one-time code, or password stored with PBKDF2 hashing. Each user sees only the websites of their own organisation, or websites they were granted as a team member. Deleting Consent Records is limited to the account owner or a team Admin.
- Access control (API): consent-data endpoints require a valid session for the website; requests that change data require a CSRF header; inputs are checked for size and format.
- Secrets: signing keys and API secrets are stored as encrypted Cloudflare secrets, not in source code, and are rotated after any suspected exposure.
- Internal access: access to production data is limited to named staff who need it for support or maintenance, uses individual accounts with multi-factor authentication on Cloudflare, and is bound by confidentiality.
- Physical security: no ConsentBit-operated servers; physical security is provided by Cloudflare's data centres (ISO 27001, SOC 2 Type II).

2. Pseudonymisation and data minimisation

- IP addresses are shortened before storage (IPv4 /24, IPv6 /48).
- No names, emails or account identifiers of Visitors are collected.
- The Consent ID is random, scoped to one website, and not linked to identity.
- Deletion logs keep only a one-way hash of the Consent ID.

3. Integrity

- All traffic to and from the banner script, the API and the dashboard uses HTTPS (TLS 1.2 or higher).
- Each Visitor-record deletion is logged (who, when, how many records).
- Changes to the production service are made through version control and reviewed before deployment.

4. Encryption

- In transit: TLS 1.2 or higher.
- At rest: Cloudflare D1 and KV encrypt all stored data at rest (AES-256).

5. Availability and recoverability

- Hosted on Cloudflare's global network, which provides DDoS protection and redundancy.
- The banner keeps working, and keeps blocking scripts until consent, if the consent API is unavailable.
- The database recovery capabilities are point-in-time restore of the Cloudflare D1 database to any moment in the last 30 days (Time Travel, Workers Paid plan).

6. Retention enforcement

- An automated job runs twice a month (on the 1st and 15th) and removes Consent Records past their retention period from the active database, and logs each run.
- Records of removed websites are deleted within 30 days.

7. Incident management

- Written incident-response procedure with a 48-hour customer notice target and an incident log (section 9).

8. Regular testing and review

- Yearly review of these measures (section 4.10).
- Security review of code changes affecting Personal Data; periodic security audits of the service, with critical findings fixed before release.
- Sub-processor security reviewed yearly (certifications and terms).

Annex III: Sub-processors (authoritative list)

Sub-processor	Services	Personal data	Processing locations
Cloudflare, Inc. 101 Townsend St, San Francisco, CA 94107, USA	Hosting banner/API Workers; D1 database; KV storage.	Consent Records. Data subjects: Visitors to Customer websites.	Consent Records: Cloudflare D1 database, EU jurisdiction; retention archive: Cloudflare D1 database, Western Europe. Banner delivery and request routing: Cloudflare's global network. Support access: ConsentBit staff in the United States.

Transfer safeguards for Cloudflare: Cloudflare's Data Processing Addendum (version 6.4, effective 3 April 2026), incorporated by reference into Cloudflare's Self-Serve Subscription Agreement, so it applies to ConsentBit's account without a separate signature. Cloudflare, Inc. is certified under the EU–US, UK and Swiss–US Data Privacy Frameworks; its DPA falls back to the EU SCCs (with the UK Addendum and Swiss changes) if that certification lapses.

Services used only for ConsentBit customer account administration, billing, account emails or product analytics are described in the Privacy Policy. They do not receive Visitor Personal Data and are not Sub-processors under this DPA.