DATA PROCESSING AGREEMENT

Brainstorm Force US LLC

SureContact · Sigmize · OttoKit · ZipWP · SureFeedback · SureCookie

August 2026

Subject to our Terms of Service ("Terms of Service" or "Agreement"), we (Brainstorm Force US LLC, "BSF") process Personal Data on behalf of users of our services ("You" or "Customer"), for which we act as the processor under applicable Data Protection Laws, and our Customers act as the controllers. That Personal Data is referred to as "Controller Data," as further described below.

"Data Protection Laws" means any and all privacy, security and data protection laws and regulations that apply to the Controller Data processed by BSF under this Agreement, including, as applicable, the GDPR, Member State laws implementing the GDPR, the UK GDPR, and the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (collectively, the "CCPA"), each as amended.

"GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

"Personal Data" means any information relating to an identified or identifiable natural person, or that is otherwise deemed personal information or personal data (or similar variations of those terms) under Data Protection Laws.

This Data Processing Agreement ("DPA") explains BSF's data protection obligations and rights as a processor of the Controller Data, as well as those of our Customers as the controllers. Other than the data protection obligations and rights in this DPA, the Agreement you have with BSF will cover everything else.

Note on corporate relationship: Brainstorm Force US LLC holds a majority ownership interest in SureCart Inc., which operates the SureCart platform under a separate Data Processing Agreement. This DPA is entered into exclusively with Brainstorm Force US LLC and governs only the products listed in Schedule 1 (SureContact, Sigmize, OttoKit, ZipWP, and SureFeedback).

1. Role of the Parties

With regard to the processing of Controller Data, BSF is the processor and the Customer is the controller. For purposes of this DPA, references to "processor" and "controller" shall be replaced with any corresponding terms with analogous meanings defined under Data Protection Laws (for example, "service provider" and "business" under the CCPA).

2. Scope of Processing

2.1 BSF shall process Controller Data on behalf of and in accordance with the instructions of the Customer as specified in Section 2.4. If BSF is legally required to process Controller Data for another purpose, BSF will inform the Customer of that legal requirement unless the law prohibits BSF from doing so.

2.2 BSF certifies that it will not:

(a) collect, retain, use, disclose or otherwise process Controller Data for any purpose other than the specific purpose of performing the services on behalf of the Customer;

(b) collect, retain, use or disclose Controller Data for a commercial purpose other than providing the services to the Customer;

(c) process Controller Data outside of the direct business relationship between Customer and BSF;

(d) combine Controller Data with any other personal data BSF collects (directly or via any third party) other than as expressly permitted for processors under Data Protection Laws; or

(e) "sell" or "share" (each as defined by the CCPA) the Controller Data.

2.3 BSF processes Controller Data for the purpose of providing its software-as-a-service products to Customers. Controller Data consists of personal data relating to data subjects who interact with or are managed within a Customer's instance of an applicable BSF product, which may include the Customer's customers, contacts, subscribers, employees or other users. The type of Controller Data processed and the duration of processing correspond to the duration of the Agreement as further described in Schedule 1.

2.4 The instructions of the Customer are in principle conclusively stipulated and documented in this DPA. Individual instructions which deviate from the stipulations of this DPA or which impose additional requirements shall require BSF's written agreement. BSF will promptly inform the Customer if, in BSF's opinion, an instruction from the Customer infringes applicable Data Protection Law.

2.5 Customer shall comply with its obligations under Data Protection Laws. The Customer is responsible for the lawfulness of the processing of Controller Data. In case third parties assert a claim against BSF based on the unlawfulness of processing Controller Data or any other violation of Data Protection Law by Customer, the Customer shall release BSF from any and all such claims.

2.6 Customer agrees that BSF may depersonalise (including through deidentification) the Controller Data or aggregate data in a way which does not permit the identification of a natural person, and use the data in this form for purposes of designing, further developing, optimising, and providing its services to the Customer as well as to other users of the service, provided that if such data is "deidentified" (as defined under Data Protection Law), BSF will take reasonable measures designed to ensure such data cannot be associated with a natural person and will commit to maintaining this data in deidentified form. The parties agree that Controller Data rendered depersonalised or aggregated as described in this Section is no longer classified as Controller Data under this DPA.

3. Personnel Requirements

3.1 BSF shall require all personnel engaged in the processing of Controller Data to treat Controller Data as confidential.

3.2 BSF shall ensure that natural persons acting under BSF's authority who have access to Controller Data shall process such data only on BSF's instructions.

4. Security of Processing

4.1 BSF shall implement appropriate technical and organisational measures to protect Controller Data in accordance with Data Protection Laws, taking into account the state of the art, implementation costs, and the nature, scope, circumstances, and purposes of processing, as well as the different likelihood and severity of risk to data subjects.

4.2 BSF shall establish prior to the beginning of processing and maintain throughout the term the technical and organisational measures set out in Schedule 2, and shall implement measures designed to ensure that processing of Controller Data is carried out in accordance with those measures.

4.3 BSF shall have the right to modify technical and organisational measures during the term of the Agreement, provided that any such modifications do not materially reduce the overall level of protection afforded to Controller Data.

5. Sub-processors

5.1 Customer hereby authorises BSF to engage sub-processors to provide its services to the Customer. In general, no authorisation is required for contractual relationships with service providers that are not actively processing Controller Data but are only concerned with the examination or maintenance of data processing procedures or systems, even if access to Controller Data cannot be excluded, as long as BSF takes reasonable steps to protect the confidentiality of the Controller Data.

5.2 BSF shall make available to the Customer the current list of sub-processors for each product at the URL listed in Schedule 3. Customers should check that page regularly for updates. Through that page, BSF shall provide notice to the Customer of any intended changes concerning the addition or replacement of sub-processors. An objection may only be raised by the Customer for important reasons which must be substantiated. If the Customer does not object within 14 days after the notification date, the Customer's right to object to that engagement lapses. If the Customer objects, BSF is entitled to terminate the Principal Agreement on reasonable notice.

5.3 The agreement between BSF and its sub-processors shall impose on the latter the same data protection obligations as those incumbent on BSF under this DPA. If BSF engages a sub-processor outside the European Economic Area, BSF shall ensure appropriate transfer safeguards are in place before transferring Controller Data to that sub-processor.

6. Support Obligations

6.1 BSF shall provide assistance to the Customer pursuant to its obligations as a processor under Data Protection Laws, including, as applicable, Article 28 of the GDPR.

6.2 Customer will inform BSF of any request to exercise data subjects' rights that BSF must assist with, and will provide the information necessary for BSF to comply. Upon receiving such notice and information, BSF shall to a reasonable extent support the Customer with technical and organisational measures in fulfilling the Customer's obligation to respond to requests for exercising data subjects' rights.

6.3 BSF shall notify the Customer without undue delay after becoming aware of any breach of the security of Controller Data that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Controller Data (each, a "Security Incident"). The notification shall contain a description of the following if and to the extent known by BSF:

(a) the nature of the breach, indicating, as far as possible, the categories and approximate number of affected data subjects and the categories and approximate number of affected personal data records;

(b) the likely consequences of the Security Incident; and

(c) the measures taken or proposed by BSF to remedy the Security Incident and, where appropriate, measures to mitigate its potential adverse effects.

6.4 The above details may be provided in multiple notifications as information becomes available. In the event that the Customer is obligated to inform supervisory authorities and/or data subjects of a Security Incident, BSF shall, at the request of the Customer, assist the Customer in complying with those obligations.

6.5 BSF will take appropriate steps to remediate the cause of any Security Incident and will use commercially reasonable efforts to cooperate with the Customer with respect to the investigation and remediation of any Security Incident, which may include providing assistance to enable Customer to notify and cure an alleged violation of Data Protection Law related to a Security Incident.

7. Deletion and Return of Controller Data

Upon termination of the Principal Agreement, BSF shall delete all Controller Data, unless BSF is obligated by law to further store such Controller Data. Nothing in this Section requires deletion of Controller Data that has been anonymised or aggregated such that it no longer constitutes Controller Data under this DPA.

8. Evidence and Audits

Customer has the right to take reasonable and appropriate steps to ensure that BSF processes Controller Data in accordance with the requirements of this DPA as specified in this Section 8.

8.1 BSF shall ensure that the processing of Controller Data is consistent with this DPA, comply with all obligations applicable to it as a processor under Data Protection Law, and provide the same level of privacy protection as is required by Data Protection Law. BSF shall notify Customer within five business days after making a determination that it cannot meet its obligations under the CCPA with respect to Controller Data.

8.2 BSF shall document the implementation of the obligations under this DPA in an appropriate manner and provide the Customer with appropriate evidence at the Customer's reasonable request.

8.3 At the Customer’s reasonable request, BSF shall demonstrate compliance with the obligations under this DPA by submitting an opinion or report from an independent authority (such as an auditor) or a suitable certification by IT security or data protection audit relating to BSF’s data processing systems.

9. Transfer of Controller Data

In processing Controller Data as part of the Principal Agreement, BSF may transfer Controller Data outside the European Union, the United Kingdom, or Switzerland. When BSF does so, it will use the applicable mechanism outlined below.

9.1 For Controller Data Transferred Outside of the European Union

For any Controller Data transferred outside the European Union to a Third Country, the parties agree to be bound by the Standard Contractual Clauses as further set out in Schedule 4.

"Standard Contractual Clauses" means the standard contractual clauses for the transfer of personal data to processors in third countries according to Decision (EU) 2021/914 of the EU Commission of 4 June 2021.

"Third Country" means a country that the EU has not recognised as providing an equivalent level of protection for personal data as the EU.

9.2 For Controller Data Transferred Outside of the United Kingdom

For any Controller Data subject to the UK GDPR that is transferred outside the United Kingdom to a Third Country, the parties agree to be bound by the UK Addendum as set out in Schedule 4.

"UK Addendum" means the Addendum to the Standard Contractual Clauses issued by the UK Information Commissioner, in force 21 March 2022.

"UK GDPR" means the GDPR as incorporated into United Kingdom law by the Data Protection Act 2018 and amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, each as amended, superseded, or replaced. For purposes of any Controller Data subject to the UK GDPR, references to the GDPR in this DPA will be replaced with references to the UK GDPR.

9.3 For Controller Data Transferred Outside of Switzerland

For any Controller Data subject to Swiss DP Law that is transferred outside of Switzerland to a Third Country, the parties agree to be bound by Swiss SCCs as set out in Schedule 4.

"Swiss DP Law" means the Swiss Federal Act on Data Protection (as updated from time to time).

"Swiss SCCs" means the applicable standard data protection clauses issued, approved or otherwise recognised by the Swiss Federal Data Protection and Information Commissioner.

10. Liability

10.1 Each party's liability under this DPA shall be subject to the limitations set out in the Principal Agreement, except where Applicable Data Protection Law does not permit such limitation with respect to data subject rights.

11. Term

11.1 This DPA shall remain in force for as long as BSF processes Controller Data on behalf of the Customer under the Principal Agreement.

11.2 Provisions that by their nature should survive termination (including Sections 9 and 12) shall survive expiration or termination of this DPA.

12. General

12.1 This DPA shall be governed by the laws of the State of Delaware, United States, except to the extent Applicable Data Protection Law requires otherwise. The parties submit to the exclusive jurisdiction of the courts of Delaware, except as required by the Standard Contractual Clauses in Schedule 4.

12.2 This DPA may only be amended by written instrument signed by authorised representatives of both parties, or by BSF updating the DPA on its legal page with at least 30 days' prior notice.

12.3 If any provision is held unenforceable, the remaining provisions shall remain in full force and effect.

12.4 This DPA, together with the Schedules and the Principal Agreement, constitutes the entire agreement between the parties regarding the processing of Controller Data and supersedes all prior agreements on the same subject matter.

SCHEDULE 1

Processing Details per Product

This Schedule sets out the specifics of personal data processing for each BSF product, as required by Article 28(3) GDPR.

1A. SureContact

Processor: Brainstorm Force US LLC · Servers: United States

Subject Matter	Operation of the SureContact CRM and email marketing platform, including contact management, email campaign delivery, marketing automation workflows, and audience segmentation.
Nature of Processing	Collection, storage, use, transmission, and deletion of contact data and marketing consent records on behalf of the Customer.
Purposes	Contact management and CRM operations; email marketing campaign delivery; marketing consent and preference management; contact segmentation and tagging; automation workflow triggering; activity logging and audit trails; CSV import/export operations.
Types of Personal Data	Contact PII: email, first/last name, phone, company, job title, birthdate, gender, name prefix/suffix. Consent and preference data: email marketing consent status, opt-in timestamp, consent source, unsubscribe details. Behavioural data: email open/click history, activity logs. Timezone and language preferences.
Categories of Data Subjects	Contacts managed by the Customer in SureContact (the Customer's customers, leads, subscribers, or other contacts). The Customer's own users and team members accessing the platform.
Retention	Contact data: retained until the Customer requests deletion. Activity and change logs: 90-day rolling retention, then automatically deleted. Unsubscribe records: retained indefinitely to honour opt-outs.

Controller Responsibility	The Customer is responsible for establishing the lawful basis for processing its contacts' data within SureContact.

SureContact Note: The Customer is solely responsible for the lawful basis on which it processes contact data, for obtaining any required consents from contacts, and for ensuring that custom webhooks and SMTP configurations route contact data only to third-party destinations with adequate data protection. BSF does not control destinations configured by the Customer.

1B. Sigmize

Processor: Brainstorm Force US LLC · Servers: United States

Subject Matter	Operation of the Sigmize A/B split testing and website visitor analytics platform. Customers install Sigmize on their websites to run controlled experiments, measure conversion performance, and optionally generate visitor heatmaps and session recordings.
Nature of Processing	Collection, storage, use, and deletion of: (a) Sigmize account data for registered customers; and (b) visitor behavioural data collected on the Customer's website via the Sigmize script.
Purposes	Customer account management and authentication; delivery and measurement of A/B and multivariate experiments; visitor behaviour analytics (anonymised by default); optional session recording and heatmap generation; product analytics and improvement; error monitoring.
Types of Personal Data — Account Holders	First name, last name, email address; workspace identifiers and usage data; billing information (processed via SureCart).
Types of Personal Data — Website Visitors	DEFAULT (anonymised): Experiment assignment data, page event data, conversion events, aggregated behavioural metrics. IP addresses are NOT collected or stored by default. OPTIONAL — Screen Recordings / Heatmaps (when enabled by Customer): Session replay data, cursor movement, clicks, scroll depth, and page interaction sequences. The Customer must ensure appropriate visitor consent is in place before enabling this feature.

Categories of Data Subjects	Sigmize customers (workspace owners and team members). Visitors to the Customer's website(s) on which the Sigmize script is installed.
Retention	Account data: retained until explicit deletion request. Application and event logs: 90-day rolling retention, then deleted.
Controller Responsibility	The Customer is responsible for establishing the lawful basis for processing visitor data collected via Sigmize, including obtaining appropriate consent before enabling the optional screen recording/heatmap feature.

Sigmize Note: In its default configuration, Sigmize does not collect visitor IP addresses and processes only anonymised behavioural data. The optional screen recording/heatmap feature captures more granular visitor data. By enabling this feature, the Customer warrants that it has implemented an appropriate consent mechanism (e.g., a cookie/tracking consent banner) on its website. BSF is not responsible for verifying the adequacy of the Customer's consent mechanism.

1C. OttoKit

Processor: Brainstorm Force US LLC · Servers: United States

Subject Matter	Operation of the OttoKit no-code workflow automation platform, enabling customers to create automated workflows connecting third-party applications and services.
Nature of Processing	Collection, storage, use, and deletion of: (a) user account data for registered OttoKit customers; and (b) workflow execution history logs retained temporarily for debugging and retry purposes only.
Purposes	User account creation, authentication, and management; workflow automation execution and orchestration; workflow execution history logging (solely for enabling customers to rerun failed steps and debug errors); transactional email and push notification delivery; product analytics and improvement; error and security monitoring.

Types of Personal Data — Account Holders	Username, email address, first name, last name, display name. WhatsApp mobile number (if provided for notifications). Hashed password, registration date. IP addresses (login history), user agent. Timezone preferences, temporary verification codes.
Types of Personal Data — Workflow History	Workflow execution logs may contain personal data depending on the data sources and actions the Customer configures. Not all workflows involve personal data — this is determined entirely by the Customer's workflow configuration. Workflow history is automatically and permanently deleted per the plan-tiered schedule below.
Categories of Data Subjects	OttoKit account holders (the Customer's team members). Any individuals whose data the Customer routes through OttoKit workflows (if applicable — determined solely by the Customer).
Retention	Account data: retained while active; sessions and verification tokens expire automatically. Workflow execution history — automatically deleted per subscription plan: Free plan: 3 days; maximum under any plan: 30 days. No workflow history is retained beyond 30 days under any plan.
Controller Responsibility	The Customer is solely responsible for the lawful basis under which personal data flows through their OttoKit workflows.

OttoKit Note: OttoKit is a general-purpose automation platform. Whether personal data flows through a Customer's workflows depends entirely on how the Customer configures those workflows — many automations involve no personal data at all. Workflow logs are retained only temporarily (maximum 30 days, automatically deleted per plan tier) solely for the Customer's own debugging and retry use. Customers must apply data minimisation when building workflows that handle personal data and must not route special categories of personal data (Article 9 GDPR) through OttoKit without implementing appropriate additional safeguards.

1D. ZipWP

Processor: Brainstorm Force US LLC · Servers: United States

Subject Matter	Operation of the ZipWP AI-powered WordPress website builder platform, including user account management, AI-assisted site generation, WordPress site creation and hosting, custom domain provisioning and DNS management, cloud server management, email address verification, and real-time notifications.

Nature of Processing	Collection, storage, use, transmission, and deletion of: (a) user account and team data; (b) AI prompt data shared with third-party AI providers; (c) WordPress site data including files, databases, and backups; (d) custom domain registration and

	DNS records; and (e) email addresses submitted for deliverability verification.
Purposes	Account management and authentication (including 2FA and social login); AI-based website content generation from user-provided prompts; WordPress site creation, hosting, and management; cloud server provisioning and deployment; custom domain registration and DNS management; SSL certificate provisioning; email address deliverability verification at signup; AI credit verification and token issuance; real-time notifications and broadcasting; transactional email delivery; product analytics and improvement; bot prevention and form security; error monitoring and exception tracking.
Types of Personal Data — Account Data	Identity: name, email, avatar, company. Authentication: hashed password, encrypted 2FA secrets, OAuth tokens (Google). Team data: team ID, team UUID, platform identifier, credit usage counts. Preferences: language, timezone. Activity: last login, signup source, lifecycle stage, user events. Session data: IP address, user agent, session tokens (120-minute expiry). Bot prevention data: visitor IP, browser fingerprint, challenge tokens.
Types of Personal Data — AI Prompts	Business descriptions, site prompts, and content instructions provided by the Customer. These are shared with third-party AI providers (OpenAI, Groq AI, Google Gemini) solely for content generation. Customers should not include personal data of third parties in AI prompts unless necessary.
Types of Personal Data — Site Data	WordPress site configuration, content, uploaded media, and any end-user data the Customer's hosted site collects. Site backups (database and files). Custom domain registration data: domain name, registrant contact (name, email, address, phone), nameservers, DNS records. Server credentials and deployment metadata for cloud-hosted sites. End-user data on Customer sites is processed under the Customer's instructions as Controller.
Categories of Data Subjects	ZipWP customers (website owners). End users of websites built and/or hosted on ZipWP (if

	applicable — Customer is Controller for that data).
Retention	Activity logs: 365 days, then automatically deleted. User accounts: retained until deletion request. Sites: retained until user deletes. Sessions: expire after 120 minutes of inactivity.
Controller Responsibility	The Customer is responsible for establishing the lawful basis for any personal data processed through its ZipWP account, including data submitted to AI content generation features. Where the Customer uses ZipWP's cloud hosting and custom domain features, the Customer is Controller for all end-user data collected by the hosted WordPress site and for the domain registrant contact data submitted to the registrar.

ZipWP Note: BSF shares user-provided business descriptions and AI prompts with OpenAI, Groq AI, and Google Gemini for content generation only. Customers are advised not to include unnecessary personal data in AI generation prompts. ZipWP's cloud hosting feature provisions WordPress sites on Customer-selected infrastructure providers (including Vultr, Hetzner, InterServer, Velia, and Leapswitch), managed through RunCloud. Custom domains are registered through OpenProvider, with SSL certificates issued by Let's Encrypt. Email addresses are verified at signup using Clearout to confirm deliverability. BSF Group Services (SureContact, Sigmize, OttoKit) are not used in connection with ZipWP.

1E. SureFeedback

Processor: Brainstorm Force US LLC · Servers: Finland (EU)

Subject Matter	Operation of the SureFeedback visual feedback and website annotation platform, enabling customers to collect contextual feedback on websites and design mockups from team members and clients, and to deliver email notifications and campaigns related to feedback activity.
Nature of Processing	Collection, storage, use, transmission, and deletion of: (a) user account data for registered SureFeedback customers and their invited collaborators; and (b) feedback content, annotations, file attachments, and design mockups submitted through the platform.
Purposes	User account management and authentication; website and design mockup feedback collection; comment and annotation management; file and screenshot storage; team collaboration and notification delivery; email campaign and transactional email delivery; email marketing and subscriber management; user avatar retrieval; Figma design import; CRM webhook forwarding; issue tracker integration (GitHub, Jira); webhook-based integrations; product analytics and conversion tracking; bot detection; error and performance monitoring.

Types of Personal Data	Account data: name, email address, profile picture, Google OAuth tokens (if used), MD5-hashed email addresses (transmitted to Gravatar for avatar retrieval). Feedback content: comments, annotations, point-click coordinates, file attachments (screenshots, mockup images, PDFs), Figma design exports. Email data: email addresses, email content, delivery metadata (for both transactional notifications and campaign emails). Activity data: workspace and organisation identifiers, session tokens, activity logs. CRM data: first name, last name, email, signup source, creation timestamp (forwarded to SureContact via webhook).
Categories of Data Subjects	SureFeedback account holders (workspace owners and team members). Invited collaborators and clients who leave feedback through shared links.
Retention	Account data: retained until explicit deletion request. Feedback content and attachments: retained until the Customer deletes them or the account is terminated. Session tokens and cached data expire automatically.
Controller Responsibility	The Customer is responsible for establishing the lawful basis for processing feedback data within SureFeedback, and for ensuring that collaborators and clients are appropriately informed before being invited to provide feedback.

SureFeedback Note: SureFeedback's primary application server is hosted in Finland (EU) by Hetzner. Object storage uses both Amazon S3 (eu-north-1, EU) and Cloudflare R2 (global Anycast). Email delivery uses Amazon SES in two regions: us-east-1 for campaign emails and us-west-2 for transactional emails; campaign email processing involves a transfer of email data to the United States. SureFeedback injects a script on the Customer's website to enable the feedback overlay interface. This script is only active when the website is accessed through a SureFeedback review link and does not affect general website visitors. Gravatar (Automattic) receives MD5-hashed user email addresses to retrieve avatar images. Customers may optionally connect GitHub or Atlassian Jira to create and sync issues from feedback comments; when enabled, feedback data is transmitted to the Customer's chosen issue tracker. The Customer is responsible for ensuring that custom webhook destinations and connected issue trackers have adequate data protection. BSF does not control destinations or integrations configured by the Customer.

1F. SureCookie

Processor: Brainstorm Force US LLC · Servers: Bavaria, Germany (EU)

Subject Matter	Operation of the hosted services supporting the SureCookie consent plugin on the Customer's WordPress site: discovery of cookies and tracking scripts on pages the Customer submits for scanning, and resolution of a visitor's approximate location from their IP address so that the correct consent rules apply to that visitor.
Nature of Processing	Collection, storage, use, and deletion of: (a) site registration data for the Customer's website; (b) page URLs submitted for automated crawling and the scan results produced from them; and (c) visitor IP addresses submitted for location resolution.

Purposes	Site registration and identification; automated crawling of Customer-supplied page URLs to discover cookies and tracking scripts; storage of scan results for display in the Customer's WordPress admin; resolution of a visitor's location from their IP address so that the consent rules for their country apply; licence validation on paid plans.
Types of Personal Data — Administrator	WordPress administrator email address, sent once per site on the first scan together with the site URL. Page URLs and the site base URL of the Customer's website. Where the Customer completes the plugin's onboarding form, the administrator's first name, last name, email address and site domain are also sent to BSF's marketing endpoint.
Types of Personal Data — Website Visitors	Visitor IP address, transmitted unmasked for location resolution. The lookup resolves city, region and country level; the plugin reads back only the country. No other visitor data is transmitted, and nothing is transmitted on an ordinary page view.
Categories of Data Subjects	The Customer's own WordPress administrator. Visitors to the Customer's website, at the point they interact with the consent banner.
Retention	For the term of the Principal Agreement. Scan results and cookie instances: retained for as long as the site remains registered, and deleted on written request or on termination. Visitor IP addresses submitted for location resolution: cached against the lookup result for 7 days, then expired. They are not written to BSF's request logs.
Controller Responsibility	The Customer is responsible for establishing the lawful basis for processing visitor data through SureCookie, for the page URLs it submits for scanning, and for the content of its own cookie notice and consent records.

SureCookie Note: SureCookie is a plugin installed on the Customer's own WordPress site, and five calls leave that site. Site registration runs once per site on the first scan and sends the site URL and the WordPress administrator email address. Scan execution runs on a manual or scheduled scan and sends the page URLs to be crawled, the site base URL and a scan bypass token; it carries no visitor data and no administrator email. Location resolution sends a visitor's raw, unmasked IP address when that visitor interacts with the consent banner and the local country cache holds no answer for them, and it also runs per view where a Pro Geographic Targeting rule is set to anything other than worldwide. That IP is resolved against a MaxMind GeoLite2 database file held on BSF's own server, so no third party receives it and MaxMind is not a sub-processor. The lookup resolves city, region and country level, and the plugin reads back only the country. The IP is cached against its result for 7 days and then expires, and it is not written to BSF's API request log, which records the request path without its query string and logs the address of the calling website's server rather than the visitor's. Licence validation on paid plans sends a licence identifier, signature and plan type as request headers and carries no personal data. The plugin also fetches the blocking catalog from library.surecookie.com; that request carries no personal data. Requests to library.surecookie.com are served through Cloudflare before reaching BSF's servers in Bavaria, Germany. Nothing leaves the Customer's site on an ordinary visitor page view in the free plugin. The consent log itself stays on the Customer's site and is never transmitted to BSF; the visitor IP written to that log is anonymised as it is written by WordPress core, which zeroes the last octet of an IPv4 address and truncates an IPv6 address to the /64.

SCHEDULE 2

Technical and Organisational Security Measures

The following security measures apply to the processing of Controller Data under this DPA and may be updated in accordance with Section 4.3 of the main Agreement.

1. Encryption

1.1 Personal data is encrypted at rest using industry-standard encryption. Passwords are hashed using industry-standard one-way hashing algorithms and are never stored in plain text or shared with third parties.

1.2 API tokens and keys are cryptographically hashed. Sensitive credentials (including SMTP passwords and OAuth tokens) are encrypted at rest.

1.3 All data in transit is encrypted using industry-standard transport layer encryption. Unencrypted connections are not supported.

2. Access Controls

2.1 Role-based access control (RBAC) limits employee access to personal data to those with a documented business need.

2.2 Multi-tenant architecture enforces strict data isolation — no Customer can access another Customer's data.

2.3 BSF maintains commercially reasonable access control procedures designed to limit access to Controller Data, including secure authentication, session management, and additional verification for sensitive account changes.

3. Infrastructure and Availability

3.1 Primary application servers are located in the United States. Encrypted backups are performed regularly and stored securely with restricted access.

3.2 CDN and DDoS mitigation services protect availability and filter malicious traffic. Application performance and errors are monitored using dedicated observability tools.

4. Organisational Measures

4.1 Personnel with access to personal data are subject to confidentiality obligations. Access to production systems is restricted, logged, and requires justification.

4.2 BSF maintains an incident response plan and tests breach notification procedures. Security patches are applied promptly and dependencies are monitored for known vulnerabilities.

4.3 Sub-processors are subject to contractual data protection obligations at least as protective as this DPA.

SCHEDULE 3

Sub-processor Lists

The current list of sub-processors for each BSF product is maintained at the following URL, organised by product. BSF will update this page and provide notice of any material changes in accordance with Section 5.2 of this DPA. Customers should check this page regularly.

https://brainstormforce.com/legal/sub-processors

This page lists sub-processors for: SureContact, Sigmize, OttoKit, ZipWP, and SureFeedback.

Note: Where a sub-processor is located outside the European Economic Area, BSF shall ensure that appropriate transfer safeguards (such as the Standard Contractual Clauses) are in place before transferring Controller Data to that sub-processor.

SCHEDULE 4

Standard Contractual Clauses

For Controller Data Transferred Outside of the European Union:

For transfers outside of the European Union, the parties agree to be bound by the Standard Contractual Clauses. The Standard Contractual Clauses (linked below) are incorporated into this Data Processing Agreement:

Standard Contractual Clauses:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN

There are certain sections of the Standard Contractual Clauses that require population or selection, which are set out in the following table:

Section Reference	Concept	Selection by the Parties
Clause 7	Docking Clause	The option under clause 7 shall not apply
Section II, Clause 9	Approval of Sub-processors	Option 2: GENERAL WRITTEN AUTHORIZATION
Section IV, Clause 17	Governing law	The laws of Ireland
Section IV, Clause 18(b)	Choice of forum and jurisdiction	The courts of Ireland
Annex I.A	List of Parties	Data Exporter: The Customer, as identified in the Principal Agreement. Data Importer: Brainstorm Force US LLC, 340 S Lemon Ave #5769, Walnut CA 91789, United States; legal@brainstormforce.com.
Annex I.B	Description of Transfer	Categories of data subjects, categories of personal data, and purposes as described in Schedule 1 for the applicable product. Frequency: continuous. Nature: collection, use, storage. Duration: for the term of the Principal Agreement.
Annex I.C	Competent Supervisory Authority	Irish Data Protection Commission
Annex II	Technical and Organisational Measures	See Schedule 2 of this DPA
Annex III	List of Sub-processors	See Schedule 3 of this DPA

For Controller Data Transferred Outside of the United Kingdom:

For transfers outside of the United Kingdom, the parties agree to use the UK Addendum. The UK Addendum (linked below) is incorporated into this Data Processing Agreement:

UK International Data Transfer Addendum:
https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf

Section Reference	Concept	Selection by the Parties
Clause 7	Docking Clause	The option under clause 7 shall not apply
Clause 11	Redress	The option under clause 11 shall not apply
Section II, Clause 9(a)	Approval of Sub-processors	Option 2: GENERAL WRITTEN AUTHORIZATION
Section IV, Clause 17	Governing law	The laws of England and Wales insofar as transfers are governed by UK Data Protection Laws
Section IV, Clause 18(b)	Choice of forum and jurisdiction	The courts of England and Wales shall have exclusive jurisdiction
Annex I.A	List of Parties	As set out above in the EU SCC table
Annex I.B	Description of Transfer	As set out above in the EU SCC table
Annex I.C	Competent Supervisory Authority	The UK Information Commissioner's Office (ICO)
Annex II	Technical and Organisational Measures	See Schedule 2 of this DPA
Annex III	List of Sub-processors	See Schedule 3 of this DPA
Section 19 of UK Addendum	End of UK Addendum when the Approved Addendum changes	Neither party may end this UK Addendum per Section 19, except as set forth in the Principal Agreement

For Controller Data Transferred Outside of Switzerland:

For transfers outside of Switzerland, the parties agree to use the Standard Contractual Clauses outlined above, with the following modifications to account for Swiss law:

Amended Provision	Modification

Clause 13 and Annex I.C — Competent Supervisory Authority	The Swiss Federal Data Protection and Information Commissioner (FDPIC) shall be the competent supervisory authority
Processing standard	The parties agree to abide by the GDPR standard in relation to all processing of Controller Data that is governed by Swiss DP Law
Interpretation of the term 'Member State'	The term 'Member State' in the Standard Contractual Clauses will not be interpreted to exclude data subjects who habitually reside in Switzerland from initiating legal proceedings in Switzerland in accordance with Clause 18(c) of the Standard Contractual Clauses
References to the 'GDPR'	References to the 'GDPR' in the Standard Contractual Clauses will be understood as references to the Swiss Federal Act on Data Protection insofar as the transfer of Controller Data is subject to the Swiss Federal Act on Data Protection

END OF DATA PROCESSING AGREEMENT

Brainstorm Force US LLC · August 2026