# Flashbrand Privacy and Security Policy

April 10th, 2021

This document sets out the Privacy and Security Policy (the "Policy") of Flashbrand, Inc. (the "Company," "Flashbrand," "we," or "us"). It describes how we protect your data and respect your privacy.

## I. Overview.

Flashbrand understands that privacy and data security is important to you and your organization (individually and collectively referred to herein as "you" or "your") and we are committed to respecting your privacy when you visit any website operated by the company, including www.flashbrand.me (collectively, the "Sites"), use any of our mobile applications, and/or otherwise access our services via a direct or indirect connection to the internet or sign up for and use any of our products or service offerings via our website or otherwise, including, without limitation the Flashbrand platform (collectively, the "Services").

The following information in this Policy is designed to help you better understand what information we gather from you and through your use of any of our Services, how we use and disclose this information, who we might share this information with, and to describe generally what security steps Flashbrand takes.

This Policy is incorporated into and subject to the terms of any End User Subscription Agreement, Free Trial Agreement, or other agreement entered into between Flashbrand and you and/or your organization (either via clickthrough acceptance or otherwise) (collectively, the "Use Agreements"). This Policy applies to all Sites operated or controlled by the Company and all Services provided, however it does not apply to any third-party site linked to our Site or recommended or referred by our Site or any third party service used in the provision of the Services to you (including, without limitation, third party sites used for sign-in to our Services).

## II. Data Collection and Use

### A. Overview and Definition of Personally Identifiable Information; Additional Information Collected by Flashbrand.

*By visiting our Websites, accessing or using our Services, or interacting with any aspect of our business, you accept the terms of this Privacy Policy and expressly consent to our collection, use, and disclosure of data, including Personal Data, provided to or otherwise received by us for the purposes and in the manner described in this Privacy Policy (and the Client Agreement when applicable).*

Client Data

Clients and Authorized Users routinely submit Client Data to Flashbrand when using the Services. Client Data is governed by the Client Agreement. Client Data may include Account Information, Hosted Data, Sync Data, or any Client Data otherwise defined in the Client Agreement.

If you have any questions about your Personal Data with respect to Client Data, please contact your Company representative.

Account Information (Including Personally Identifiable Information)

In providing our Services or otherwise interacting with you through your use of our Sites or our Services, we may collect your personally identifiable information ("PII") as well as other information we receive as described in this Policy. PII includes personal information such as:

- Employee First Name
- Employee Last Name
- Employee email address
- Employee ID
- Gender
- Profile Photo URL
- Feedback data (unstructured)
- Performance Management Data (unstructured)
- Employment Status (e.g., Active/Inactive)
- Employment Type (e.g., Full-Time, Part-Time, Contract)
- Tenure
- Hiring Date
- Job Title
- Job Location
- Division / BU / Legal Entity
- Department Name
- Manager Employee ID
- Manager Name
- Manager Email Address
- HRBP Employee ID
- HRBP Name
- HRBP Email Address
- anything else a user provides to us that can in any manner identify the user

Additionally, PII collected by Flashbrand includes such information that you upload or otherwise submit to Flashbrand, including, but not limited to any content you share publicly in connection with your use of the Services, information provided to Flashbrand in connection with communications related to support or other issues you contact us about, or billing information. When you create or establish an account with us, we collect and store such information about you and your company, and we use this information for reasons including to provide access and permissions necessary to facilitate the Services, to communicate with your regarding your account and/or the Services, and to monitor and improve the Services.

Hosted Data

Through its Services, the Company provides technology services used to support certain internet-based solutions, including internet-based communications and applications (including "mobile apps") as well as other information that users input, post, upload, or store via use of the Services. As a result, the Company's hosting services store and transmit information about our customers, their business, as well as information collected or inputted by those businesses (the "Hosted Info"). Hosted Info may include PII and other information that belongs to you and/or your employees or other service providers.

Except to the extent necessary to render the Services to you, the Company does not purposefully access any Hosted Info. For example, if you input information as text feedback, our Service passively receives such information and normally only accesses or reviews such information to the extent necessary to provide the Services to you (and provide any related support of the Services) and you agree that such access is permissible

for all purposes. You are solely responsible for the content of all information you post, upload, store, display, transmit, or submit on the Services, including Personal Information, and the consequences thereof. Flashbrand is not responsible and will not be liable for the information you disclose while using the Services.

Third Party Authenticator and Application Information

If you log-in to our Services using a Third Party Authenticator (as defined in Section 5 below) or if you utilize a third party application that you integrate with the Services (a "Third Party Application"), we may receive and collect information relating to your credentials with such Third Party Authenticator or Third Party Application, as applicable, including service log-in, email, profile picture, and/or other information transmitted by such Third Party Authenticator or Third Party Application to us

Technical Data and Syncing Information

In addition, when you use the Services, we may collect certain information related to you by automated means, including (1) technical data about your computer or device, such as IP address, operating system, browser and platform information, and device type and (2) usage data and statistics relating to your interactions with our Services. We use the foregoing technical data to facilitate updates and support, and to improve our Services.

We make other tools available to sync information with our Services, and may also develop additional features that allow you to sync information stored via our Services to other third-party services used by you or your organization (each an "Additional Platform"). If you use the Service and integrate your receipt of Services with one or more additional Platforms, we will receive and collect information, potentially including PII, from the Additional Platform for the purpose of important information between our Services and the Additional Platform, and you consent to such syncing and agree that the transfer of all such information that is distributed to an Additional Platform is permissible.

B. Methods of Information Collection of Information, Including Collection of PII.

General Use

When you use the Services or otherwise interact with our Site, your information, including your PII, Hosted Info, and any other information you input, post, display, transmit, or submit via use of our Services may be collected and stored by us, and such information is available to other users accessing the Services in your company. Information that you provide through your direct interactions with our Site, or through email or written correspondence, telephone calls, or web-based forms or otherwise may be collected and stored in our general business practices, and to facilitate the provision of Services and related support.

Cookies

We also may place "cookies" (a small file) or similar technologies on your hard drive during your access to any of our Sites or use of our Services to help us identify the number of unique visitors to our Sites, learn what our users' technology preferences are, monitor the functionality of our Sites and/or Services, help with authentication/login and otherwise improve our Services. We may also use "local storage," a feature of your browser, to retain information locally regarding your usage to improve our Services. If you do not wish to have cookies placed on your computer or do not wish for us to use "local storage" you may adjust your web browser settings accordingly. If adjustment is not feasible, you may elect to refrain from using our Services or accessing our Sites. Please be aware that restricting cookies may impede your ability to use our Site or our Services or certain features of our Site or our Services.

For additional information about cookies and your ability to opt out of certain aspects of their functionality, you can visit applicable resources including http://www.allaboutcookies.org, http://youronlinechoices.eu/ (European Union), https://helpx.adobe.com/flash-player/kb/disable-localshared-objects-flash.html (flash cookies).

Log Files & Third-Party Analytics

Like most internet-enabled services, we use log files on the server side. The data held in log files includes information such as your IP address, browser type, e-mail application, Internet service provider ("ISP"), referring/exit Web pages, computer platform type, date/time stamp, and user activity. The Company uses server log data to analyze trends, administer the Services offered through our Sites and otherwise administer our Sites and the Services.

The software enabling the Sites and the Services has associated log and temporary files that are stored on Company controlled servers. These files may store your account information, preference settings, system notifications as well as other data necessary to enable you to participate on the Site and/or use the Services. Your information may also exist within regularly performed server backups.

We use third-party analytics services to provide us with information relating to your use of the Services, including information relating to your usage of the Services, performance data, and related information, to help us better understand how our Services perform on different devices and under different circumstances.

## C. Use of Your Data, Including PII

Client Data will be used by Flashbrand in accordance with Client's instructions, including any applicable terms in the Client Agreement and Client's use of Services functionality, and as required by applicable law.

We use your data, including PII, to create your account and to (i) communicate with you about Services you have purchased from Flashbrand, (ii) offer you additional products and services, (iii) allow use of the Sites and the applicable Services you have purchased, (iv) process service requests, (v) provide access to secure areas of the Sites and/or secure aspects of the Services, (vi) send invoices for our Services and process payments related thereto, and (vii) ensure compliance with applicable laws, including intellectual property laws. We also use PII to the extent necessary to enforce all applicable Use Agreements, monitor adherence to all applicable Use Agreements, and to attempt to prevent and/or detect fraud, as well as to allow third parties to carry out technical, logistical or other functions on our behalf as provided in this Policy.

For example, your account information is stored on servers controlled by the Company and if you forget your log-in password, you will be asked to enter your e-mail address on record with the Company in order to gain access to the Site or Service (as applicable). Moreover, we collect additional information from you when you provide us with on-line comments or feedback via our Site or via our Services or post information about yourself or others to a Site or via the Services. This information, if any, is available to others accessing the Site or Service (as applicable). We work to process and maintain accurately the information that you share with us and will comply with all applicable law and use appropriate efforts to allow you the ability to change or modify your user information in order to enhance your ability to use our Sites and the Services you have purchased.

Additionally, when you purchase or subscribe to a Service, we collect your contact information (such as your address) and may collect your financial information (such as your credit/debit card information). To facilitate our provision of the Services, we may also receive Hosted Info (as defined below) and host such information as described below in Section D. We use the information you provide only to complete that Service order or to otherwise fulfill the Service. We do not share this information with unaffiliated parties except to the extent necessary to complete that transaction. If we have trouble processing an order, we use the applicable portions of the PII to contact you. For clarification, we may use third party vendors to process payment transactions

(the “Payment Processors”) and you agree to such use and understand that the terms and conditions (and privacy and security policies) of such vendors shall govern and control for all purposes with respect to all applicable payment processing transactions related to your purchases. By using our Services, you consent to the processing of your data by such Payment Processors as applicable, and you understand and agree that we have no liability for the errors of delays of our Payment Processors.

### D. Security Measures

Substantially all information Flashbrand receives from you or via your use of any Services is copied, stored and managed through computer servers owned or controlled by Flashbrand or our vendors. We use appropriate security based on the category and sensitivity of the data at issue, and we endeavor to employ security techniques commensurate with industry norms to protect your data, including PII, and other Hosted Info from unauthorized access by users inside and outside the organization. However, you should be aware that perfect security does not exist on internet-enabled systems; third parties may unlawfully or improperly intercept or access transmissions, personal information, or private communications. As such, we cannot make complete assurances that a security breach will not occur that may expose your PII or other information to others.

For example, the Flashbrand servers are not located at Flashbrand but rather are managed and located at a third-party Infrastructure-as-a-Service provider (an “IAAS”). We have taken appropriate steps to choose a professional IAAS provider using adequate and appropriate security measures to protect against unauthorized access, alteration, disclosure, or destruction of your information commensurate with the category and sensitivity of the information, but we cannot guarantee the performance of the IAAS provider, its security measures, or the actions or inactions it takes in the future. By using our Services, you consent to the processing of your data, including PII, by such IAAS providers

Flashbrand endeavors to only collect as much PII as required to provide customers with our Service and meet our legal obligations. In addition, we will use commercially reasonable efforts to store and encrypt PII in a secure location, encrypt passwords, and utilize a minimum of 128-bit Secure Socket Layer (SSL) certificates to protect transactions to and from our Site(s) if sensitive information is transmitted.

Your user account related to the Services is also protected by a password for your privacy and security. Initially, you are assigned a random password but are given the option to change it if you choose. You need to ensure that there is no unauthorized access to your account, your PII and/or your Hosted Info by selecting (if you so choose) and protecting your password appropriately and limiting access to your computer (or other device) and browser by signing off after you have finished accessing your account. Additionally, we may use third party sign-in providers to authenticate users of our Services, such as Google Signin and OneLogin (the “Third Party Authenticators”). You understand that your information (including PII) may be made available to and stored by such Third Party Authenticators and by using our Services, you consent to the processing of your data by such Third Party Authenticators.

### E. Sharing of Information.

We may share your information as described in this Policy, including to our service providers as described herein, or as otherwise consented to by you. As a matter of policy, we will not sell or rent information about you and we will not disclose your PII or Hosted Info in a manner inconsistent with this Policy except as required by law or government regulation. We cooperate with law enforcement inquiries, as well as other third parties, to enforce laws such as those regarding intellectual property rights, fraud and other personal rights. WE CAN (AND YOU AUTHORIZE US TO) DISCLOSE ANY INFORMATION ABOUT YOU, INCLUDING YOUR PII OR OTHER HOSTED INFO, TO LAW ENFORCEMENT, OTHER GOVERNMENT OFFICIALS, OR ANY OTHER THIRD PARTY THAT WE, IN OUR SOLE DISCRETION, BELIEVE NECESSARY OR APPROPRIATE IN CONNECTION WITH AN INVESTIGATION OF FRAUD, INTELLECTUAL PROPERTY INFRINGEMENT, OR OTHER ACTIVITY THAT IS ILLEGAL OR MAY EXPOSE US, OR YOU, TO CRIMINAL OR CIVIL LIABILITY.

In any case, sharing or disclosing data should respect:

- Client's Instructions. Upon Client's request, Flashbrand may share and disclose Data in accordance with Client's instructions, including any applicable terms in the Client Agreement and Client's use of the Services functionality, and as required by applicable law. Pursuant to the Client Agreement, Client Data is generally treated as the confidential information of Client unless stated otherwise.
- Client Access. Administrators, Authorized Users, and other Client representatives and personnel may be able to access or restrict access to data. For example, a Client may use the admin control to modify a role permission on viewing certain data.
- Displaying the Services. When an Authorized User submits data on the Services, it may be displayed to the Client and other Authorized Users in the same environment. For example, an Authorized User's name may be displayed with their profile accessible to the Client and other Authorized Users in the same Company. Authorized Users are solely responsible for all data posted, uploaded, stored, sent, or submitted on the Services, including Personal Data, and the consequences thereof. Flashbrand is not responsible and will not be liable for the data disclosed on the Services.
- Rendering the Services. Flashbrand employees may have access to data on a need to know and confidential basis to the extent necessary to render the Services and related support for the Services.
- Third Party Service Providers. Flashbrand engages third parties to support the delivery of the Services ("Third Party Service Providers"). Flashbrand may share Personal Data, with Third Party Service Providers (e.g. cloud computing services, data storage) to the limited extent necessary to let them perform business functions and services for us or on our behalf in connection with the provision of the Services; provided that such Third Party Service Providers process data in a manner consistent with this Policy and applicable data protection laws and will not use or disclose Personal Data for any other purpose.
- Third Party Services. Client may enable or permit integrations with or use of Third Party Services in connection with the Services. When enabled, Flashbrand may share certain data with such Third Party Services as requested to effectuate the integration. Third Party Services are not owned or controlled by Flashbrand and third parties that have been granted access to data may have their own policies and practices for its collection and use.
- Changes to Flashbrand Business. If Flashbrand engages in a merger, acquisition, bankruptcy, dissolution, reorganization, sale of some or all of its assets or stock, financing, public offering of securities, acquisition of all or a portion of its business, a similar transaction or proceeding, or steps in contemplation of such activities (e.g. due diligence), Flashbrand may share or disclose data in connection therewith, subject to standard confidentiality obligations.
- Aggregated or De-identified Data. If any data is aggregated or de-identified so it is no longer reasonably associated with an identified or identifiable natural person, Flashbrand may use or disclose such aggregated or de-identified data for any purpose. For example, Flashbrand may share aggregated or de-identified data with prospects or partners for business or research purposes, such as statistical analysis, to research trends and predictive analysis, or to develop or improve the Services.
- Enforcement of Agreements. Flashbrand may disclose data to ensure compliance with and enforce Client Agreements and any other contractual or legal obligations with respect to the Services and its business.
- Protection of Rights. Flashbrand may disclose data to protect and defend its rights and property, including intellectual property rights, and to ensure compliance with applicable laws and enforce third party rights, including intellectual property and privacy rights.
- Legal Compliance. If Flashbrand is compelled by law, such as to comply with a subpoena, court order, or other lawful process, or in response to a lawful request by public authorities to meet national security or law enforcement requirements, Flashbrand may disclose data if it reasonably believes disclosure is in accordance with or required by any applicable law, regulation, or legal process.
- Safety and Security. Flashbrand may disclose data to protect Client and Authorized Users safety and security; and to protect the safety, security, and property of Flashbrand and its employees, agents, representatives, and contractors.

- Client Consent. Flashbrand may disclose Client data to third parties when having Client express consent to do so.

In addition, if Flashbrand undergoes a business transaction such as a merger, acquisition, dissolution, or a sale of some or all of its assets, we may share, disclose, or transfer your information to the successor organization during such transition or in contemplation of such transition.

F. Retention.

As required by law, Flashbrand will not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held. Therefore, Flashbrand will retain Client Data in accordance with a Client's instructions, including any applicable terms in the MSA and Client's use of the Services functionality, and as required or permitted by applicable law.

Flashbrand may retain Other Information and any data pertaining its Clients, including Personal Data, for as long as the Authorized User account is active and thereafter for as long as necessary for the purposes described in this Policy, including for the period of time needed to pursue our legitimate business interests, provide Client with the Services, conduct audits, resolve disputes, comply with contractual obligations (including but not limited to Client Agreements), and comply with (and demonstrate compliance with) legal obligations.

## III. Data Controller and Data Processor

Data protection and privacy laws in certain jurisdictions differentiate between the "controller" and "processor" of data. In general, Client is the controller of Client Data. In general, Flashbrand is the processor of Client Data and the controller of Other Information.

## IV. Avoidance of Sensitive Information; Use of Services by Children.

We will not intentionally collect or maintain, and request that you do not provide, sensitive personal information, including any information regarding or constituting any social security or other government-issued identification numbers, financial account numbers, consumer reports or background checks, biometric data, personal account access, or information relating to medical or health conditions, your race or ethnic origins, political opinions, your religious or philosophical beliefs, or other such information.

Use of our Site and our Services are not designed for or directed to children under the age of 13, and we will not intentionally collect or maintain information about anyone under the age of 13 (or anyone under the age of 16 in the Europe Economic Area). Any parent who believes we may have collected personal data from a child under those ages can submit a request that it be removed by contacting us at support@flashbrand.me.

## V. Your Rights and Choices Regarding Your Data.

Depending on the jurisdiction you are located in and additional factors, you have rights pertaining to your data, including the right to opt out of certain treatment of your information. You can contact us directly regarding the exercise of these rights, or about other questions you have relating to the handling of your information.

## A. Data Choices / Communications

To stop receiving promotional communications from us, you can opt out by using the unsubscribe mechanism in the promotional communication you receive or by changing the email preferences in your account. Note that

regardless of your email preference settings, we will send you transactional and relationship messages regarding the Services, including administrative confirmations, order confirmations, important updates about the Services, and notices about our policies.

For information relating to cookies used for tailored advertising from participating companies, see the consumer opt-out pages for the Network Advertising Initiative and Digital Advertising Alliance, or if you are located in the European Union, visit the Your Online Choices site.

To opt out of allowing Google Analytics to use your data for analytics or enrichment, see the Google Analytics Opt-out Browser Add-on.

In addition to updating your account information by logging into your account at any time, you have the right to access, update, and/or delete your personal information as follows:

- To terminate your account, please contact us at support@flashbrand.me. Please note that, (1) even after you terminate your account, content you have shared with third parties via the Services may still be visible to others and (2) we may retain your data for as long as we have a legitimate purpose to do so (and provided such retention is otherwise in accordance with applicable law), including to assist with legal obligations, resolve disputes, and enforce our agreements.

- To request to access, update, correct, or delete your data, please email support@flashbrand.me or write by mail to Flashbrand, Inc., Attn: Privacy Policy Agent One Sansome Street, Suite 3500, San Francisco, CA 94104.

## B. Rules and Consents Applicable in Particular Jurisdictions

### California Users

A user of the Services can prevent any future disclosures for direct marketing purposes of his or her PII, at no charge, by exercising his or her “opt out” rights by using the “opt out” procedures described below:

1. Send an email to: support@flashbrand.me, or
2. Send mail to the following postal address:

Flashbrand, Inc.
Attn: Privacy Policy Agent
One Sansome Street
Suite 3500
San Francisco, CA 94104
USA

Because the Company provides its California users with the ability to exercise his or her “opt out” rights as described above, pursuant to Section 1798.83(c)(2) of the California Civil Code, the Company is in compliance with the California “Shine the Light” law.

### Users Outside the United States

Flashbrand is headquartered in San Francisco, California. However, we have endeavored to structure our operations to facilitate the storage of the data you provide on servers located within European Economic Area (“EEA”). Nevertheless, our customer support operations and other aspects of our communications with you may be provided to some extent by personnel located outside of the EEA, including in the United States. If you

are using the Services from outside the United States, you consent to the transfer, storage, and processing of your data in and to the United States or other countries. Accordingly, although we attempt to minimize any such transfer and storage, personal data collected in Switzerland and the European Economic Area ("EEA") may be transferred and stored outside those areas. To the extent such transfers and storage occur, we will do so in accordance with applicable law.

Your data may also be processed outside of Switzerland and the EEA by our service providers, including to process transactions, facilitate payments, and provide support services as described in this Policy. We have entered into agreements with our service providers that restrict and regulate their processing of your data on our behalf. By submitting your data or using our Services, you consent to this transfer, storage, and processing.

Subject to and to the extent provided by applicable law, you may also have the right to request various changes or responses relating to how we process your information. The following summarizes certain rights you may have relating to your information. These rights are subject to restrictions under European data protection law and, subject to the exemptions in that law, may only apply to certain types of information or processing.

1. We need your consent for some of the ways we may use your information, such as for marketing or the processing of certain special categories of information about you. You can remove that consent at any time.
2. You can ask us to confirm if we are processing your information and if we are, you can ask for access to that information and various details regarding that processing, including, but not limited to, who we have shared the information with, the transfers of your information, the source of your information other than you, and your rights to complain to the applicable supervisory authority.
3. You can ask us to correct your information if it is inaccurate, to delete certain information, or to restrict or, in some circumstances cease, our use of it.
4. You can ask us to help you move certain of your information to other companies.

You also have a right to object to us processing your information in certain circumstances, and you can ask us to stop processing your information, although in certain circumstances we may not be able, or may not be required, to do so (including, for example, if there are outstanding contracts between us, if applicable law requires that we keep the information, or if the information).

If you have questions about these rights or would like to exercise or discuss any of your rights under applicable law, please feel free to contact us (1) at our support email address, support@flashbrand.me, or (2) by mail at Flashbrand, Inc., Attn: Privacy Policy Agent, One Sansome Street, Suite 3500, San Francisco, CA 94104.

## VI. Enforcement.

The Company will actively monitor its relevant privacy and security practices to verify adherence to this Policy. Any individual service provider that the Company determines is in violation of this Policy will be subject to disciplinary action up to and including termination of service.

We reserve the right to change, modify, or update this Policy, in whole or in part, in our sole discretion at any time. Any changes to this Policy will be posted on this website. If we make material changes to this Policy, we will notify End Users via email, through a notification posted on the Services, or as required by applicable law, and we will include a summary of the key material changes. Unless stated otherwise in our notification, changes will become effective on the date of posting. As permitted by applicable law, your continued use of the Services after the effective date of any changes will constitute your agreement to follow and be bound by the revised Policy.

If you have any questions or concerns regarding our Privacy Policy or our handling of your information, please do not hesitate to contact us (including our designated personal information protection manager) (1) at our support email address, support@flashbrand.me, or (2) by mail at Flashbrand, Inc., Attn: Privacy Policy Agent, One Sansome Street, Suite 3500, San Francisco, CA 94104.