MyBrandForce Privacy Policy and Notice

Effective date: 19-Jan-2024

MyBrandForce is revolutionizing retail execution by connecting innovative brands with the power of an unprecedented, on-demand workforce. Our services platform allows brands of all sizes to perform scalable field services and acquire real-time observational data from retail locations across the country. MyBrandForce Brand Agents use our digital platform execute retail assignments ("missions") and capture real-time observational data ("mission content").

Privacy and data protection is central to what we do, and this Privacy Policy and Notice ("Policy" or "Notice") describes how MyBrandForce collects, uses, discloses, and otherwise processes personal information described in "Scope," as well as the rights and choices individuals have regarding such personal information. This Notice applies to the extent we process personal information on our own behalf, as a controller or business.

For information about the privacy choices you have regarding your personal information, review 8. Your Privacy Choices, as well as 14. Additional Information for Residents in Certain Jurisdictions, which includes additional information about privacy rights for residents of specific jurisdictions such as Colorado, Connecticut, Utah, and Virginia. If you are a resident of California, please also refer to Section 14.3. for information about the categories of personal information we collect and your rights under California privacy laws.

Your use of our Services (defined below), and any dispute over privacy, is subject to this Notice and our Terms of Use, including their applicable limitations on damages and the resolution of disputes.

1. Scope

Except as otherwise noted below, this Notice applies to the personal information that MyBrandForce processes as a controller related to:

- our "Services," which include our mobile applications, websites, and other online services (and any feature thereof) and other products and services we make available to customers and partners.
- individuals that apply to become a MyBrandForce brand agent.
- individuals who are hired and paid as a MyBrandForce brand agent.
- individuals that register for or participate in our webinars and other events.

- current, former, and prospective independent contractors, customers, vendors, and partners
- individuals who are subscribed to receive news, information, and marketing communications from us; and
- individuals that communicate with us or otherwise engage with us related to our Services.

In addition, except where expressly stated otherwise, this Policy does not apply to the extent we process personal information on behalf of our clients as a "processor" or "service provider" under applicable privacy laws ("Client Data"). Our processing of Client Data is subject to the terms of our contracts with each client, who is the "controller" or "business" under applicable privacy laws for the data that we process on their behalf. In such cases, MyBrandForce's clients are responsible for ensuring that there is an appropriate legal basis for the processing of Client Data by MyBrandForce, and that appropriate notice has been provided, and any necessary consent has been obtained, for the processing of such data.

Additional Notices. In some cases, additional or supplemental privacy notices (each an "additional notice") may be provided and will apply to certain personal information collected and processed by us in connection with specific Services that we provide. The additional notice will control to the extent there is a conflict with this Policy, with respect to your personal information that is subject to that notice.

2. How we collect personal data

We may collect personal information directly from individuals, automatically, and from third parties when such data relates to the use of our Services or other interactions with us.

Data provided by users. The personal information we may collect from you depends upon how you use our Services or otherwise interact or engage with us, but includes:

- *Registration and profile information.* When you register for an account in connection with our Services, or we provide you with account login credentials to access our Services, we may collect certain personal information from you, such as your name, phone number, date of birth, email address, and zip code as well as any personal information that you otherwise submit to us through your account.
- *Background check information (brand agents):* This includes information submitted during the brand agent application process, such as driver history or criminal record (where permitted by law), license status, known aliases, prior addresses, and right to work. This information may be collected by an authorized vendor on MyBrandForce's behalf.
- *Payments.* When you register to receive payment through the Services, we collect payment or banking information to process your payments. This information may be collected by an authorized vendor on MyBrandForce's behalf.
- *Identity verification photos:* This includes photos of users (such as, selfies) and/or their government issued identifications (such as, driver's license or passports). Such photos may be used to verify a user's identity, such as through facial verification technologies. Please see the section titled "How we use personal data" for more information regarding how user photos are used for safety and security purposes, including identity verification.
- *Demographic data:* We may collect demographic data about users, such as birth date/age, gender, or occupation, when required for certain MyBrandForce services or programs, such as Services involving alcohol. We may also collect demographic data – such as age group,

education level, language skills, and household composition – through user surveys, and use this information to offer MyBrandForce products and services that are likely to be of interest to you.

- *Communications and interactions.* When you text, email, call, or otherwise communicate with us and with members of our team, we may collect and maintain a record of your contact details, communications, and our responses. We also maintain records of communications regarding information you provide to us related to any customer support requests.
- *Survey responses.* When you provide answers to the surveys we publish in connection with our Services, we may collect such survey responses, including but not limited to information regarding demographics, your food and drink consumption and preferences, your workplace, your education level and your opinion about products and services. Participation in our surveys is completely voluntary. You may choose not to answer any survey.
- *Events and other requests.* We may also collect personal information about your participation in our events and other requests you submit to us related to our Services. For example, if you register for or attend an event that we host or sponsor, we may collect information related to your registration for and participation in such event. When you contact us via text, social media, email, sign up for our mailing lists, or otherwise request information from us, we collect and maintain records of your requests, including through forms you may complete on our website.

Data created during use of our services. We automatically collect personal information related to your use of our Services and interactions with us and others, including information we collect automatically (e.g., using cookies and pixel tags), as well as information we derive about you and your use of the Services. Such information includes:

- *Location data (brand agents).* We collect precise or approximate location information from brand agents' mobile devices if they enable us to do so via their device settings. MyBrandForce collects such data any time the mobile app is running in the foreground (app open and on-screen) or background (app open but not on-screen). Brand agents may use the MyBrandForce apps without enabling collection of location data from their mobile devices. However, this may affect certain features in the MyBrandForce apps. For example, a brand agent who has not enabled location data will not be able to claim or complete a mission.
- *Usage data:* We collect data about how users interact with our services. This includes access dates and times, app features or pages viewed, browser type, and app crashes and other system activity.
- *Device data:* We collect data about the devices used to access our services, including the hardware models, device IP address or other unique device identifiers, operating systems and versions, software, preferred languages, advertising identifiers, device motion data, and mobile network data.

Data from other sources. We may collect personal information about you from third party sources, such as public databases, joint marketing partners, social media platforms or other third parties.

- Lead and prospect information from third parties about prospective independent contractors or customers that may be interested in our Services. We may also engage with third parties to enhance or update our customer information.

- Users participate in our referral programs. For example, when a user refers to another person, we receive the referred person's data from that user.
- Users or others providing information in connection with claims or disputes.
- MyBrandForce business partners through which users create or access their MyBrandForce account, such as payment providers, social media services, secure document management services, or apps or websites that use MyBrandForce's APIs or whose APIs MyBrandForce uses.
- Vendors who help us verify users' identity, background information, and eligibility to work, or who screen users in connection with sanctions, anti-money laundering, or know-your-customer requirements.
- Publicly available sources
- Law enforcement officials, public health officials, and government authorities
- Marketing service providers or data resellers whose data MyBrandForce uses for marketing or research.

3. How we use personal data

MyBrandForce uses data to enable reliable and convenient mission execution and other products and services. We also use such data:

- to provide our services
- to enhance the safety and security of our users and services
- for customer support
- for research and development
- to enable communications between users
- for marketing and advertising
- to send non-marketing communications to users
- in connection with legal proceedings

We use the data we collect:

- *To provide our services.* MyBrandForce uses data to provide, personalize, maintain, and improve our services. This includes using data to:
  - create/update accounts.
  - enable mission data collection and other services/features.
  - match available brand agents to missions needing services. Users can be matched based on availability, location/proximity, user settings/preferences and other factors such as likelihood to accept a mission based on their past behavior or preferences.
  - offer features that facilitate the use of our services by those with disabilities.
  - enable dynamic pricing, in which mission prices or other fees are determined based on factors such as estimated time and distance, predicted route, estimated traffic, and the current number of users requesting or providing services.
  - process payments
  - personalize users' accounts. For example, we may present brand agents with training and/or mission opportunities based on their training or mission completion history.
  - perform necessary operations to maintain our services, including troubleshooting software bugs and operational problems.

MyBrandForce performs the above activities on the grounds that they are necessary to fulfill the terms of our agreements with users, are compatible with such uses, or on the grounds that they are necessary for purposes of MyBrandForce's and its users' legitimate interests.

- *Safety and security.* We use data to help maintain the safety, security, and integrity of our services and users. This includes:
    - verifying users' identity and eligibility to provide mission services, including through reviews of background checks, to help prevent use of our services by unsafe brand agents.

      We may use facial recognition technology to process user profile photographs, identification photographs, or other user-submitted photographs to prevent identity-borrowing or use of our services by unauthorized brand agents.

      We may also use photos taken by users ("selfies") to verify that users are wearing branded clothing or products as required for the mission using object verification technology.

      Brand agents may be required to provide their age and an image of their government issued identification to verify their eligibility to participate in alcohol-related or other age-restricted missions.

    - using brand agent location information, and communications between brand agents, to identify mission fees earned or induced through fraud. For example, if we determine that a brand agent, individually or in cooperation with another brand agent, is delaying a mission completion to drive up the fee for the mission, we will take disciplinary measures against all parties involved.
    - using device, location, user profile, usage, and other data to prevent, detect, and combat other types of fraud. This includes identifying fraudulent accounts or uses of our services, preventing use of our services by unauthorized brand agents, verifying user identities in connection with certain payment methods, and preventing and combating unauthorized access to users' accounts. In some cases, such as when a user is determined to be abusing MyBrandForce's referral program or has submitted fraudulent documents, such behavior may result in automatic deactivation, or in the European Union or where otherwise required by law, deactivation after human review. To object to such a deactivation, please contact MyBrandForce customer support.

  MyBrandForce performs the above activities on the grounds that they are necessary to fulfill the terms of our agreements with users, and/or for purposes of the legitimate safety and security interests of MyBrandForce, our users and members of the public.

- *Customer support.* MyBrandForce uses the information we collect (which may include call recordings) to provide customer support, including to investigate and address user concerns and to monitor and improve our customer support responses and processes.

MyBrandForce performs the above activities on the grounds that they are necessary to fulfill the terms of our agreements with users or for purposes of MyBrandForce's legitimate interest in monitoring and improving its customer support services.

- *Research and development.* We use data for testing, research, analysis, product development, and machine learning to improve the user experience. This helps us make our services more convenient and easier-to-use, enhance the safety and security of our services, and develop new services and features.

  MyBrandForce performs the above activities on the grounds that they are necessary for purposes of MyBrandForce's legitimate interests in improving and developing new services and features.

- *Enabling communications between users.* For example, a brand agent may message or call an operations manager to confirm a mission location or details.

  MyBrandForce performs the above activities on the grounds that they are necessary to fulfill the terms of our agreements with users.

- *Marketing and Advertising.* MyBrandForce may use data to market its services and those of MyBrandForce partners. This may include:

  - Sending emails, text messages, push notification, and in-app messages or other communications marketing or advertising MyBrandForce products, services, features, offers, promotions, sweepstakes, news, and events.

    This may include using location, mission history, device data and usage data to send marketing communications that are personalized based on users observed or inferred interests and characteristics. For example, we may send push notifications or in-app messages offering bonuses or promo for locations where brand agent has previously completed missions. See the MyBrandForce *Terms of Use* for information on how to opt out of receiving communications from MyBrandForce.

  - Displaying MyBrandForce advertising on third party apps or websites. This includes using location, mission history, device data and usage data, and sharing hashed email addresses and device or user identifiers with advertising partners (such as Facebook and TikTok), to personalize such ads to users' interests.

  - Measuring the effectiveness of MyBrandForce's ads, and of third-party ads displayed in MyBrandForce's apps or in connection with our services.

    MyBrandForce performs the above activities on the grounds that they are necessary for purposes of MyBrandForce's legitimate interests in informing users about MyBrandForce services and features or those offered by MyBrandForce partners. See the 8. Your Privacy Choices for information on your choices regarding how MyBrandForce may use your data for marketing and advertising.

- *Non-marketing communications.* MyBrandForce may use data to send surveys and other communications that are not for the purpose of marketing the services or products of MyBrandForce or its partners.

MyBrandForce performs the above activities on the grounds that they are necessary to fulfill the terms of our agreements with users, or for purposes of MyBrandForce's and its users' legitimate interests in informing users about events that may have an impact on their use of MyBrandForce services.

- *Legal proceedings and requirements.* We use data to investigate or address claims or disputes relating to use of MyBrandForce's services, to satisfy requirements under applicable laws, regulations, or operating licenses or agreements, or pursuant to legal process or governmental request, including from law enforcement.

  MyBrandForce performs the above activities on the grounds that they are necessary for purposes of MyBrandForce's legitimate interests in investigating and responding to claims and disputes relating to use of MyBrandForce's services and features, and/or necessary for compliance with applicable legal requirements.

4. Data sharing and disclosure

We may disclose the personal information that we collect for the purposes described above, to provide our Services to you, to respond to and fulfil your requests, as otherwise directed, or consented to by you, and as follows:

- *Vendors and service providers.* We may disclose personal information we collect to our service providers, processors and others who perform functions on our behalf. These may include, for example, IT service providers, payment processors, analytics providers, consultants, auditors, and legal counsel.
- *Our affiliates and subsidiaries.* We may disclose personal information we collect to our affiliates or subsidiaries, who will use and disclose this personal information in accordance with the principles of this Policy, and the more specific policies.
- *Customers.* We may disclose deidentified, aggregated information regarding your use of our Services to help our business customers better understand consumer behavior. For example, we may combine and/or aggregate information or survey responses that you allow us to collect with the responses of others to produce deidentified reports. We may also create aggregated reports based upon deidentified modeled information. "Modeled information" is data based upon demographic and behavioral characteristics (e.g., gender, age, and purchasing habits) to predict what people with similar or matching characteristics would buy.
- *Third party platforms, providers, and networks.* We may disclose or make available personal information to third party platforms and providers that we use to provide or make available certain features or portions of the Services, or as necessary to respond to your requests. We may also make certain information that includes personal information available to third parties in support of our marketing, analytics, advertising, and campaign management.
- *Commercial Partners and Other Third Parties.* (i) In connection with our business, we may disclose demographic information (e.g., gender, household size, and number of children) to commercial partners and other third parties in either single or aggregate summary form and may also provide other aggregate or deidentified information to such third parties (singular summary includes demographic information about a person

without specifically identifying the person and aggregate summary includes demographic information about a group of persons without specifically identifying any person within the group); or (ii) we may also provide your personal information, with respect to some of our Services, to commercial partners and other third parties, such as retailers, brands, and partners we co-sponsor surveys with, for marketing research and analytics purposes (for example, to create models that estimate consumer preferences in the total population or to inform market segments).

- *Data contributors with respect to digital products.* In limited instances, specifically with respect to MyBrandForce's digital products, MyBrandForce combines its own digital data with the data of its customers and other third parties. To ensure the combined data can be continuously updated by all parties contributing data, the data is associated with a unique ID that is made available to all data contributors. The data made available *does not* directly identify consumers (i.e., name, email, physical address, and other directly identifying information is *not* made available to data contributors).
- *In support of business transfers.* If we or our affiliates are or may be acquired by, merged with, or invested in by another company, or if any of our assets are or may be transferred to another company, whether as part of a bankruptcy or insolvency proceeding or otherwise, we may transfer the information we have collected from you to the other company. We may also share certain personal information as necessary prior to the completion of such a transaction or corporate transactions such as financings or restructurings, to lenders, auditors, and third-party advisors, including attorneys and consultants, as part of due diligence or as necessary to plan for a transaction.
- *Compliance and legal obligations.* We may also disclose personal information to third parties to comply with our legal and compliance obligations and to respond to legal process. For example, we may disclose information in response to subpoenas, court orders, and other lawful requests by regulators and law enforcement, including responding to national security or law enforcement disclosure requirements. This may include regulators, government entities, and law enforcement as required by law or legal process. In addition, it may include certain disclosures we must make under applicable laws, such as sweepstakes and contest winners' names.
- *Security and protection of rights.* We may disclose personal information where we believe doing so is necessary to protect the Services, our rights and property, or the rights, property, and safety of others. For example, we may disclose personal information to (i) prevent, detect, investigate, and respond to fraud, unauthorized activities and access, illegal activities, and misuse of the Services, (ii) situations involving potential threats to the health, safety or legal rights of any person or third party, or (iii) enforce, and detect, investigate and take action in response to violations of, our Terms of Use. We may also disclose information, including personal information, related to litigation and other legal claims or proceedings in which we are involved, as well as for our internal accounting, auditing, compliance, recordkeeping, and legal functions.

5. Aggregate data and non-identifiable data

We may also receive, use, and disclose aggregate and other non-identifiable data related to our business and the Services for quality control, analytics, research, development, and other purposes. Some of this information may be considered "deidentified" under U.S. privacy laws (i.e., data that it is no longer linked or linkable to an identified or identifiable consumer). Where we rely on data that has been "deidentified" as defined by U.S. privacy laws, we will maintain and use such information in deidentified form and will not attempt to reidentify such information, except to determine whether our deidentification processes are reasonable and adequate or as otherwise set forth by these laws.

6. Cookies, targeting and analytics

MyBrandForce and its partners may use cookies, pixels, local storage objects, log files, APIs, and other mechanisms to automatically collect information browsing, activity, device, and similar information within our Services and to target advertising and content. We may use this information to, for example, analyze and understand how users' access and use our Services, as well to identify and resolve bugs and errors in our Services and to assess secure, protect, optimize, and improve the performance of our Services. You have certain choices about our use of cookies and tracking within the Services, as described in this section. For more information on the types of personal information we collect via cookies and similar mechanisms, please see Section 2. How we collect personal data.

- *Cookies.* Cookies are small text files that are stored on browsers or devices by websites, apps, online media, and advertisements. Some cookies allow us to make it easier for you to navigate our Services, while others are used to enable a faster log-in process, support the security and performance of the Services, or allow us to track activity and usage data within Service.
- *Pixel tags*. Pixel tags (sometime called web beacons or clear GIFs) are tiny graphics with a unique identifier, similar in function to cookies. While cookies are stored locally on your device, pixel tags are embedded invisibly within web pages and online content. We may use these, in connection with our Services to, among other things, track the activities of users, help us manage content and compile usage statistics. We may also use these in HTML e-mails we send, to help us track e-mail response rates, identify when our e-mails are viewed, and track whether our e-mails are forwarded.
- *Third-Party Analytics and Tools*. We may allow others to provide audience measurement and analytics services to us, to serve advertisements on our behalf across the internet, and to track and report on the performance of those advertisements. These entities may use cookies, pixels, web beacons and similar tools to provide reports and metrics that help us to evaluate usage of our Services and improve performance and user experiences.
- *Browser settings.* If you wish to prevent cookies from tracking your activity on our website or visits across multiple websites, you can set your browser to block certain cookies or notify you when a cookie is set; you can also delete cookies. The Help portion of the toolbar on most browsers will tell you how to prevent your device from accepting new cookies, how to have the browser notify you when you receive a new cookie, or how to delete cookies. Visitors to our Services who disable cookies will be able to browse the website, but some features may not function.

7. International transfers of data

MyBrandForce is headquartered in the United States, and has operations, entities, and service providers in the United States and throughout the world. As such, MyBrandForce may collect your personal information from the United States, and we may transfer your personal information to and process your personal information from the United States and other jurisdictions where we and our affiliates and service providers have operations. Some of these jurisdictions (including the United States) may not provide equivalent levels of data protection as compared to your home jurisdiction.

Where applicable, transfers to service providers or other third parties will be made pursuant to the recipient's compliance with the European Commission's Standard Contractual Clauses and/or the UK's International Data Transfer Addendum/ Agreement; pursuant to the consent of the individual to whom the personal information pertains; as necessary to perform a contract with that individual or in the individual's interest, or to carry out pre-contractual steps; or as otherwise permitted by applicable law.

8. Your privacy choices

We make available several ways that you can manage your privacy choices and submit privacy requests related to your personal data. These include:

- *Account information.* You can review and update some of the personal information that we maintain about you by logging into your account, where applicable, and updating your account information.
- *Push notifications.* In connection with some of our Services, we may send push notifications from time-to-time to communicate with you regarding your account and missions. If you no longer wish to receive these types of communications, you may turn them off at the device level.
- *Targeted advertising/cookie preferences.* As described in 6. Cookies, Targeting and Analytics there are several ways that you can manage your preferences for targeting cookies and advertising by us and on our website. You can review or change your preferences for many cookies and tags on our website, other than those that are necessary to operation and functionality, by adjusting your cookie settings in your browser. These preferences are browser and device specific. So, you will need to set your preferences for each browser and device you use, and if you subsequently delete or block cookies you may need to reapply these settings.
- *Marketing communications.* You can opt out of receiving marketing emails from us by using the unsubscribe link in the footer of each marketing email we send to you.
- *Text messages.* We may use the phone number associated with a specific Service to contact you with information related to your use of that Service. Such text messages are for transactional purposes only, and never for marketing of any kind. You may opt out of text messaging at any time by texting STOP to the number provided in the text or by contacting us through the information in 13. Contact Us. Residents of certain jurisdictions, including California and other U.S. states, the European Union, and the United Kingdom, have additional rights as set forth below in 14. Additional Information for Residents in Certain Jurisdictions

For more information about our privacy practices and your privacy choices, you may contact us as set forth in the 'Contact Us' section below.

9. Data retention and deletion

MyBrandForce retains user data for as long as necessary for the purposes described above, including providing its services and complying with legal obligations. The period for which we retain user data is determined by the type of data, the category of user to whom the data relates, and the purposes for which we collected the data.
The length for which MyBrandForce retains user data may further be determined by legal and regulatory requirements, purposes of safety, security, and fraud prevention, or by issues relating to the user's account such as an outstanding credit or an unresolved claim or dispute.

For example, we retain data:

- for the life of users' accounts if such data is necessary to provide our services. E.g., user profile information and credentials.
- for 7 years if necessary to comply with tax requirements. E.g., brand agents' payment or mission location information.
- for defined periods as necessary for purposes of safety or fraud prevention. E.g., we retain incomplete brand agent applications for 1 year, and rejected brand agent applications for 7 years.
- after requests for account deletion if necessary for purposes of safety, security, fraud prevention or compliance with legal requirements, or because of issues relating to the user's account (such as an outstanding credit or an unresolved claim or dispute).

Users may request deletion of their accounts at any time. MyBrandForce may retain user data after a deletion request due to legal or regulatory requirements or for reasons stated in this policy.

Users may request deletion of their account at any time through the Profile menu in the MyBrandForce app.

Following an account deletion request, MyBrandForce deletes the user's account and data, unless they must be retained due to legal or regulatory requirements, for purposes of safety, security, financial reporting, and fraud prevention, or because of an issue relating to the user's account such as an outstanding credit or an unresolved claim or dispute. Because we are subject to legal and regulatory requirements relating to brand agents, this means that we retain their account and data for the applicable statutory retention period after a deletion request.

10. Children

Protecting the privacy of young children is especially important. Our Services are not available to children under the age of 18 and we do not knowingly collect personal information from children under the age of 18. If we learn that personal information has been collected on the Services from persons under 18 years of age and without verifiable parental consent, then we will take the appropriate steps to delete this information. If you are a parent or guardian and discover that your child under 18 years of age has obtained an account on the Services, then you may alert us using the information provided in Section 13. Contact Us, and request that we delete that child's personal information from our systems.

11. Security

We have implemented safeguards intended to protect the personal information we collect from loss, misuse, and unauthorized access, disclosure, alteration, and destruction. Please be aware that despite our efforts, no data security measures can guarantee security.

12. Changes to this Policy

This Policy is current as of the Effective Date set forth above. We may change this Policy from time to time, so please check back periodically. We will post any updates to the Policy on our web site. If we make material changes to how we collect, use, and disclose the personal data we have previously collected about you, we will endeavor to provide you prior notice, such as by emailing you or posting prominent notice through on our website or within the Services.

13. Contact us

If you have questions about this Notice or our privacy practices, you may contact us by email at info@MyBrandForce.com.

14. Additional information for residents in certain jurisdictions

This section includes additional information as required under privacy laws of certain jurisdictions.

1. EEA and UK

Residents of the EEA and UK have the following rights regarding your personal information that we hold, subject to any conditions or limitations set out in applicable law:

- *Access.* You have the right to obtain information about our processing of your personal information and obtain access to and a copy of your personal information.
- *Rectification.* You may have the right to update, complete, or correct inaccuracies in your personal information.
- *Erasure.* You may have the right to have your personal information deleted.
- *Portability.* You may have the right to obtain a machine-readable copy of your personal information or to have us transfer it to another controller of your choice.
- *Restriction.* You have the right to restrict the processing of your personal information, meaning that we will not further process your personal information except to store it.
- *Withdrawal of consent.* You have the right to withdraw your consent to our processing of your personal information, without affecting the lawfulness of processing up until withdrawal.
- You also have the right to object to the processing of your personal information for direct marketing (including profiling) purposes.

Please note that some of these rights may be limited, such as where we have an overriding interest or legal obligation to continue to process the data. Please contact us using the information set out above, in Section 13. “Contact Us,” if you wish to exercise any of your rights or if you have any inquiries or complaints regarding the processing of your personal information by us.

If you are not happy with how your rights are handled, you can submit a complaint with the relevant data protection authority of your habitual residence, your place of work or the place of the alleged infringement/violation of your rights. This link will redirect you to the European Data Protection Board Website with an up-to-date list of all European Union Data Protection

Authorities: https://edpb.europa.eu/about-edpb/board/members_en. The UK authority, the ICO, can be reached here: https://ico.org.uk/.

Controller of your Information. The controller of your information is the MyBrandForce entity you or your employer has entered a contract with, or you have subscribed to or contacted.

2. United States

If you are a resident of California, please review our California Privacy Supplement for a description of your rights pursuant to California privacy laws.

Residents of other certain other US states, including Colorado, Connecticut, Utah, and Virginia, have additional rights under applicable privacy laws, subject to certain limitations, which may include:

- *Correction.* The right to correct inaccuracies in their personal information, considering the nature and purposes of the processing of the personal information.
- *Deletion.* To delete their personal information provided to or obtained by us.
- *Access:* to confirm whether we are processing their personal information and to obtain a copy of their personal information in a portable and, to the extent technically feasible, readily usable format.
- *Opt-Out:* to opt out of certain types of processing, including:
    - to opt out of the “sale” of their personal information.
    - to opt out of targeted advertising by us.
    - to opt out of any processing of personal information for the purposes of making decisions that produce legal or similarly significant effects.

You may submit a request to exercise most of your privacy rights under U.S. state privacy laws by contacting info@MyBrandForce.com. To opt out of targeted advertising by us, you can adjust your cookies settings on your device. (See Section 8. Your Privacy Choices for additional information about the privacy choices we provide and how to exercise them.) We will respond to your request as required under the applicable privacy law(s). If we deny your request, you may appeal our decision by following the directions provided to you during the request process.

3. California Privacy Supplement

This California Privacy Supplement provides California residents with additional information regarding our collection, use and disclosure of their personal information, as well as their privacy rights, under California privacy laws, including the California Consumer Privacy Act (“CCPA”).

This California Privacy Supplement does not address or apply to our handling of publicly available information or other personal information exempt under the CCPA.

Categories of Personal Information Collected and Disclosed. MyBrandForce collects the personal information described in MyBrandForce’s Privacy Notice (this document). For California users with the following disclosure requirements, such information includes these categories of personal information defined in the California Consumer Privacy Act (CCPA):

- Personal identifiers, such as your name, address, email address, phone number, date of birth, government identification number (such as social security number), driver's license information, vehicle information, and car insurance information
- Financial information, such as bank routing numbers, tax information, and any other payment information you provide.
- Commercial information, such as your trips and mission history
- Geolocation data, including precise geolocation data.
- Biometric information, such as photos used for brand agent identity verification.
- Characteristics of protected classes, such as age and gender
- Internet or network activity information, such as your IP address, type of browser, version of operating system, carrier and/or manufacturer, device identifiers, and mobile advertising identifiers
- Audio, electronic, visual, or similar information, such as audio and video recordings submitted for customer support and safety purposes; and
- Inferences drawn from the personal information listed above, such as user interests and preferences.

Sales and Sharing of Personal Information. California privacy laws define a "sale" as disclosing or making available to a third-party personal information in exchange for monetary or other valuable consideration, and "sharing" broadly includes disclosing or making available personal information to a third party for purposes of cross-context behavioral advertising. Pursuant to the CCPA, we may sell/share personal information as described below:

- With third-party analytics companies and marketing and advertising partners: identifiers, commercial information, internet and electronic network activity information, profiles, and inferences. We do this to provide and improve our Services, improve, and evaluate our marketing and advertising campaigns, and better reach individuals with relevant ads and content.
- With our commercial partners, business customers, and data partners that utilize our media products: identifiers,
- With our commercial partners, business customers, and data partners that utilize our media products: identifiers, customer records, commercial information, professional information, education information, profiles, and inferences, including certain information considered sensitive personal information under the CCPA. We do this so that these partners may better understand consumer behavior, analyze, and improve marketing and advertising campaigns, and reach consumers with more relevant ads and content.

We do not sell or share personal information (including sensitive personal information) about individuals who we know are under sixteen (16) years old.

Sources of Personal Information. In general, we may collect personal information from the following categories of sources:

- Directly from the individual Advertising networks
- Data analytics providers
- Social networks
- Internet service providers
- Operating systems and platforms
- Data brokers
- Public databases

- Joint marketing partners
- Business customers
- Affiliates and subsidiaries

Purposes of Collection, Use, and Disclosure. As described in more detail in How we use personal data and Section 4. Data sharing and disclosure or our Privacy Policy, we may collect, use, disclose and otherwise process the above personal information for the following business or commercial purposes and as otherwise directed or consented to by you:

- Services and support
- Analytics and improvement
- Customization and personalization
- Marketing and advertising
- Planning and managing events.
- Research and surveys
- Combining personal information
- Security and protection of rights
- Compliance and legal process
- General business and operational support

Retention. We retain the personal information we collect only as reasonably necessary for the purposes described above or otherwise disclosed to you at the time of collection and as otherwise necessary to comply with our legal obligations, resolve disputes, maintain appropriate business records, and enforce our agreements. In some cases, we may aggregate or deidentify information, such that it is no longer linked or linkable to you, and we may maintain such non-identifiable information indefinitely.

CCPA Rights. Under the CCPA, California residents have the following rights (subject to certain limitations):

- *Opt out of sales and sharing.* The right to opt-out of our sale and sharing of their personal information.
- *Limit uses and disclosure of sensitive personal information.* The right to limit our use or disclosure of sensitive personal information to those authorized by the CCPA.
- *Deletion.* The right to the deletion of their personal information that we have collected, subject to certain exceptions.
- *To know/access.* The right to know what personal information we have collected about them, including the categories of personal information, the categories of sources from which the personal information is collected, the business or commercial purpose for collecting, selling, or sharing personal information, the categories of third parties to whom we disclose personal information, and the specific pieces of personal information we have collected about them.
- *Correction.* The right to correct inaccurate personal information that we maintain about them.
- *Non-discrimination.* The right not to be subject to discriminatory treatment for exercising their rights under the CCPA.

Submitting CCPA Requests. California residents may exercise their CCPA privacy rights as set forth in this section.

- *Request to know/access, correct, delete and limit.* California residents may submit verifiable requests to access/know, correct, and delete their personal information

maintained by us, as well as requests to limit the use and disclosure of their sensitive personal information online by submitting a request to info@MyBrandForce.com. You may also submit a request by calling us.

If you submit a request to access/know, correct, or delete your personal information, we will take steps to verify your request by matching the information provided by you with the information we have in our records. Please complete all required fields on our webform (or otherwise provide us with this information via the above toll-free number). We will process your request based upon the personal information in our records that is linked or reasonably linked to the information provided in your request. In some cases, we may request more information to verify your request or where necessary to process it.

- *Requests to opt out.* California residents may exercise their right to opt out online by submitting an opt out request to privacy@MyBrandForce.com or by calling us. We will apply your opt out based upon the personal information in our records that is linked or linkable to the information provided in your request. In addition, our website responds to global privacy control—or "GPC"—signals, which means that if we detect that your browser is communicating a GPC signal, we will process that as a request to opt that browser and device out of sharing (i.e., via cookies and tracking tools) on our website. Note that if you come back to our website from a different device or use a different browser on the same device, you will need to opt out (or set GPC for) that browser and device as well. More information about GPC is available at: https://globalprivacycontrol.org/
- *Authorized agents.* Authorized agents may initiate a request on behalf of another individual by contacting us at privacy@MyBrandForce.com; authorized agents will be required to provide proof of their authorization and we may also require that the relevant consumer directly verify their identity and the authority of the authorized agent.
- *Financial incentives and non-discrimination.* With respect to some of our Services, we may make available certain programs or offerings that are considered "financial incentives" under the CCPA. We do not offer financial incentives that are discriminatory. You can find a description of these programs and our applicable notice(s) as required by the CCPA in the privacy policies associated with these Services. We will obtain your consent before including you in a financial incentive and you may opt out of such participation at any time.

Rights Under California Shine the Light Law. Under California's "Shine the Light" law (Cal. Civ. Code § 1798.83), California residents who provide us certain personal information are entitled to request and obtain from us, free of charge, information about the personal information (if any) we have shared with third parties for their own direct marketing use. Such requests may be made once per calendar year for information about any relevant third-party sharing in the prior calendar year. To submit a "Shine the Light" request, email us at privacy@MyBrandForce.com, and include in your request a current California address and your attestation that you are a California resident.