Capture AI Privacy Policy

Introduction

High Jump Digital Limited (trading as **Capture AI**) is a UK-based company (registered office: 71-75 Shelton Street, Covent Garden, London WC2H 9JQ, United Kingdom) providing a chatbot management platform. This Privacy Policy explains how we collect, use, disclose, and protect personal information when you interact with our websites (including **cptr.ai** and the Capture AI dashboard at **app.cptr.ai**) and services. We understand that your privacy is important and are committed to safeguarding personal data in compliance with applicable laws (including the UK/EU General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA)) . By using Capture AI, you acknowledge that your information will be handled as described in this Privacy Policy.

Please note: In this policy, "we," "us," or "our" refers to High Jump Digital Limited (Capture AI). For purposes of data protection law, we act as a **data controller** when collecting and using personal information of our customers and website visitors, and as a **data processor** (or "service provider") when processing personal information on behalf of our customers through the chatbot services. This policy covers both scenarios.

Information We Collect

We collect personal and business information in several ways:

- **Information You Provide (Account Registration and Subscription):** When you sign up for a Capture AI account or subscription, we collect information such as your name, email address, company name, and contact details. If you purchase a subscription, we (through our payment processor) collect payment information. *Note:* Payment details (like credit card numbers) are entered into the Stripe payment interface and **we do not store your credit card information on our servers** – Stripe processes these details securely in accordance with its privacy policy . We may also collect your billing address and transaction history for invoicing and record-keeping.

- **Content You Upload:** Our platform allows you to upload company-specific knowledge and documents (e.g. brochures, PDFs, text files) to train your chatbot. Any information, including personal data, contained in the content you upload will be stored on our systems. We use this content solely to enable your chatbot to respond to inquiries (i.e. to incorporate the knowledge into the chatbot's answers) and for no other purposes. You should ensure you have the right to share any personal data contained in such content. We treat uploaded documents as confidential and do not disclose them to anyone except

as needed to provide our service to you.

- **Chatbot End-User Data:** When end-users (visitors on your website) interact with a Capture AI chatbot you've deployed, the chatbot may collect personal information from those users as configured by you, the chatbot owner. **This can include identifiers and contact details provided by the end-user (e.g. name, email address, phone number), company or business information (such as company name or role), the content of the messages and conversations, and any other information you design the chatbot to request** . For example, your chatbot might ask a visitor for their name and email to create a sales lead, or it might collect feedback or answers to questions. All such data entered by end-users into the chatbot is collected and stored on our platform.

- **Automatic Data Collection (Website/App Usage):** Like most websites, we automatically collect certain information when you visit our main site or use our app. This includes technical information such as your **IP address**, browser type, operating system, device identifiers, approximate geographic location, and browsing actions. For instance, our servers may log the pages you visited or features you used, the time and date of access, and referral URLs . We collect this usage data through cookies, scripts, and other tracking technologies (see **Cookies and Tracking Technologies** below) to understand how our websites and services are being used and to improve their performance .

- **Cookies and Tracking Data:** We and our third-party analytics and advertising partners use cookies, pixels, and similar technologies to collect information about your interactions with our sites. This may include information on your browsing behavior and preferences. See **Cookies and Tracking Technologies** for more details on what is collected and how to control it.

- **Communications:** If you contact us directly (for example, by emailing support or filling out a contact form), we will receive the information you provide in those communications. This may include your name, email, the content of your message, and any attachments or other information you choose to provide.

- **Third-Party Sources:** We may receive certain information about you from third-party sources. For example, if you arrived at our site via an advertising campaign, we might receive information from the ad platform indicating which campaign or ad led you to us. We may also collect lead or business information from marketing partners or public sources (such as LinkedIn profiles or business directories) to the extent permitted by law. Any such information will be treated in accordance with this Privacy Policy and applicable law.

We do *not* intentionally collect any sensitive personal data (such as health information, biometric data, or special category data under GDPR) as part of our services. We ask that you and your

end-users refrain from submitting such sensitive information in the chatbot conversations or through our platform.

How We Use Your Information

We use the collected information for the following purposes:

- **Providing and Improving the Service:** We use personal information to set up and maintain your account, provide the features of our chatbot platform, and ensure the service works as intended. For example, we use your registration information to create your user account and authenticate you at login, and we use end-user inputs to generate chatbot responses. We may also process your information to **operate, troubleshoot, and improve our services**, such as by analyzing usage trends to enhance our chatbot features or UI . Your information helps us understand our customers' needs and make our platform better.

- **Communicating with You:** We use contact information (like your email) to communicate about your account, provide customer support, send important service updates, and respond to your inquiries. This includes sending confirmations, invoices, technical notices, updates, security alerts, and administrative messages. If you have opted-in to receive marketing communications, we may also send newsletters or promotions about new features or offerings. You can opt-out of marketing emails at any time.

- **Payment Processing:** We use the information provided during purchase (such as subscription plan details) to manage billing and payments for our services. Payment card information is processed by Stripe on our behalf, and we use the resulting payment tokens or transaction IDs to record and manage your subscriptions. We ensure that all payment processing is done securely in compliance with PCI-DSS standards through our payment provider .

- **Enabling Chatbot Functionality for End-Users:** Any personal data collected from end-users via your chatbot (e.g. a visitor's contact details or chat messages) is used *on your behalf* to facilitate the interaction. In practice, this means the data is used to generate contextually relevant responses and to create lead entries or conversation records for you. We process end-user data to deliver it to your Capture AI dashboard, so you can review conversations or follow up on leads. **Capture AI does not use the content of your end-users' chats for any purpose other than to provide the service to you** (i.e., to power the chatbot and store the data for your access) .

- **Analytics and Performance:** We use usage data (including data gathered via cookies and similar tools) to **analyze how our website and app are used**. This helps us understand user behavior on our site, such as which pages or features are most popular, so we can optimize navigation and design . We also analyze performance metrics like

response times and system load to improve the speed and stability of our platform.

- **Advertising and Marketing Analysis:** We may use third-party advertising tools (such as the Facebook Pixel or Google Ads conversion tracking) on our website. **Data collected from advertising platforms is used solely for our internal analysis of ad performance and marketing efforts** – for example, to measure how many users sign up after clicking an ad, or to understand the effectiveness of our advertisements . This helps us refine our marketing strategies and ad targeting. We do *not* sell this data or use it to identify you personally for marketing beyond our own campaigns. (For instance, Facebook Pixel allows us to record the efficacy of Facebook ads for statistical purposes, helping us improve our ad campaigns .) If we ever engage in retargeting advertising, it will be disclosed, but as of now, any advertising-related data is used only to assess and improve our own advertising and will not be shared with third parties for their independent use.

- **Aggregate Insights and Case Studies:** We may combine and anonymize data to generate aggregate insights. For example, we might calculate the total number of chatbot conversations across all our customers or the average number of leads generated in a month. Such aggregate information **contains no personally identifiable information** and cannot be linked back to any individual. We may use and share aggregate statistics or trends (e.g., “Capture AI chatbots have handled over 100,000 user questions” or “Customers saw a 20% increase in leads”) in marketing materials, on our website, or in case studies . This is done solely to illustrate the usage or effectiveness of our services, without disclosing any personal data.

- **Security and Fraud Prevention:** We process certain data as necessary to **maintain the security of our platform, protect against fraud, and enforce our terms and policies**. For example, we may use logs and identifiers to detect and prevent malicious activity or abuse of our API. If required, we will use personal information to investigate violations of our Terms of Service or to prevent illegal activities, such as detecting bots or other unauthorized access.

- **Legal Obligations:** In some cases, we need to process personal information to comply with legal or regulatory requirements. For instance, we may retain transaction records for accounting/tax purposes or use information to fulfil know-your-customer (KYC) obligations if applicable. We may also use and disclose data as required to respond to lawful requests by public authorities or court orders (see **Sharing and Disclosure** below).

We will only use your personal information for the purposes outlined above. If we need to use it for any other purpose, we will update this Privacy Policy and, if required by law, notify or request your consent.

Sharing and Disclosure

We treat your personal information with care and **do not sell your data to third parties** . We only share or disclose personal information in the following circumstances:

- **Service Providers and Partners:** We share information with trusted third-party service providers who help us operate our business and provide our services. These entities act under contractual instructions to process data on our behalf and do *not* use your personal information for their own purposes . Key service providers include:

    - **Payment Processor:** We use Stripe for subscription billing and payment processing. Your payment-related information (like credit card details) is transmitted directly to Stripe. Stripe processes your payment data in accordance with its own privacy policy and applicable security standards. We share only necessary information with Stripe (such as your email, order amount, and an ID to tie the payment to your account) and in return receive confirmation of payment. *As noted, we do not handle or store full credit card numbers on our systems* .

    - **Analytics Providers:** We utilize third-party analytics tools (e.g., **Google Analytics**) to collect data about website traffic and user interactions. These providers set cookies or similar technologies to gather usage information (such as page visits, clicks, and referring sites) . This information helps us analyze and improve our website's performance and marketing. Analytics providers may receive your truncated IP address or device ID, but we do not allow them to use this data for any purpose other than providing services to us. You can opt out of Google Analytics as described in **Cookies and Tracking Technologies** below.

    - **Chatbot Infrastructure and AI Providers:** The Capture AI chat widget and conversation engine may rely on third-party infrastructure. In particular, we use **Voiceflow** to power aspects of our chat widget interface and conversational workflow. This means that when an end-user interacts with the chatbot on your site, the chat interface and messaging backend are facilitated by Voiceflow's technology. Voiceflow may process chat interactions (e.g. receiving the user's message and sending back the bot's reply) on our behalf. We have ensured that Voiceflow, as a sub-processor, is bound to protect any personal data in the conversations and not to use it for any purpose other than delivering the chat service. Voiceflow's own privacy policy governs its handling of data in providing their services to us. (Note: We may also utilize cloud AI services for natural language processing – for example, if our platform integrates with an AI language model API – but any such integration will be configured such that your data is not retained or used by those AI providers beyond the immediate processing. In accordance with OpenAI's and similar providers' terms, input data is not used to train their models without permission .)

    - **Cloud Hosting and Infrastructure:** Capture AI is hosted on third-party cloud servers (for example, AWS or other reputable cloud providers). Personal data (including account info and chatbot conversation data) is stored in databases and servers maintained by these providers. These cloud providers act as our data processors, storing data on our behalf. They are not permitted to access or use your data except as needed for storage and maintenance . We employ encryption and strict controls with these providers to safeguard your information.

- We maintain a list of our key sub-processors (critical service providers) and can provide this list upon request. All service providers are selected for their commitment to security and privacy.

- **Within Your Organization:** Data collected by a chatbot on our platform is accessible to the customer who deployed that chatbot (and the users/admins in their Capture AI account). For example, if your company uses Capture AI, your authorized team members can log in to our dashboard to view the leads or chat transcripts collected from your website's visitors . **We do not disclose one customer's chatbot data to any other customer.** It is your responsibility as the chatbot owner to manage who on your team has access to your Capture AI account.

- **Business Transfers:** If we are involved in a merger, acquisition, sale of assets, or similar corporate transaction, personal information may be transferred to the successor or acquiring entity. We will ensure that any such transfer is subject to confidentiality and that your personal data remains protected. If a change in ownership occurs, the successor will be bound by the terms of this Privacy Policy (or you will be provided notice and an opportunity to opt-out of any new use of your information).

- **Legal Compliance and Protection:** We may disclose personal information when we believe in good faith that such disclosure is necessary to comply with a legal obligation or request. This includes responding to subpoenas, court orders, or lawful requests by government authorities. We may also disclose your information to **enforce our agreements or policies, to bill and collect amounts owed to us, to protect the rights, property, or safety of Capture AI, our customers, our employees, or others, or to investigate and defend against legal claims or allegations** . For example, if required by law enforcement or regulators, we might provide information as mandated by law. If we need to disclose data in an emergency to protect someone's safety, we will do so as allowed by law .

- **With Your Consent or At Your Direction:** We will share your personal information with third parties if you instruct us to do so or expressly consent to a specific disclosure. For instance, if you choose to integrate Capture AI with another service (such as sending captured leads to your CRM or email marketing software via an integration), we will transfer data to those services at your direction. Likewise, if we ever want to use your personal information for a purpose not covered by this Privacy Policy, we will obtain your

consent.

- **Aggregated or De-Identified Data:** As noted, we may share aggregated information that does not identify any individual (for example, publishing a trend report or total counts). This type of data is not considered personal and may be shared freely. We ensure that such aggregated data cannot reasonably be used to identify you or any other person .

Aside from the situations above, **we do not disclose your personal data to third parties for their independent marketing or business purposes**. In particular, **we do not sell or rent personal information to data brokers or advertisers** . If that policy ever changes in the future (for example, due to a business change), we would update this Privacy Policy and provide any required notices or opt-in/opt-out choices.

Data Security

We take the security of your data seriously. Capture AI implements a variety of technical and organizational security measures to protect personal information from unauthorized access, disclosure, alteration, or destruction. These measures include, for example:

- **Encryption:** We use encryption to protect data in transit and at rest wherever feasible. The web connections to our platform (both our website and the chatbot widget) are secured via HTTPS/TLS encryption. This means data (like messages and personal details) are encrypted while being transmitted between your device, end-users, and our servers. Sensitive data, such as passwords and API keys, are stored hashed or encrypted in our databases.

- **Access Controls:** We limit access to personal data to authorized personnel and service providers who have a legitimate need to know. Within our organization, employees and contractors only access user data to the extent necessary to perform their job duties (for example, customer support or technical troubleshooting). Every employee is bound by confidentiality obligations. The data collected through your chatbots is **accessible only to you and those you authorize** in your Capture AI account . Our staff will not access the content of your chatbot conversations or uploaded documents except if required for support requests or by law, and even then only with authorization and oversight.

- **Secure Infrastructure:** Our servers are hosted in secure facilities with measures such as firewalls, intrusion detection systems, and continuous monitoring. We maintain up-to-date security software and follow industry best practices to prevent unauthorized system access. Regular backups are performed to prevent data loss, and backups are secured. We also employ measures to detect and mitigate DDoS attacks and other threats.

- **Testing and Training:** We periodically test and evaluate our security measures. This includes vulnerability scanning, security assessments, and prompt installation of security patches. Our development practices incorporate security reviews. In addition, our team members receive training on data privacy and security to ensure they understand how to protect personal data.

While we strive to use commercially acceptable means to protect your personal information, **no method of transmission over the Internet or method of electronic storage is 100% secure** . Therefore, we cannot guarantee absolute security of information. However, we will continuously update and refine our security practices to meet or exceed industry standards. In the unlikely event of a data breach that affects your personal data, we will notify you and relevant authorities as required by law.

Data Retention

We retain personal information for only as long as necessary to fulfill the purposes for which it was collected, as described in this Policy, **unless a longer retention period is required or permitted by law**. In practice:

- **Account and Customer Data:** For our direct customers (account holders), we retain your personal information while your account is active and for a reasonable period thereafter. This allows us to provide the service and have sufficient information to address any issues that may arise (for example, to support account reactivation or to comply with legal obligations). If you cancel your account or your subscription expires, we may retain certain data for a period of time in backups or archives before deletion. Typically, once you terminate your relationship with us, we will either delete or anonymize personal data associated with your account after a set retention period, unless we are required to keep it longer (e.g., for legal compliance or legitimate business interests such as resolving disputes) . Information that is no longer needed is either securely deleted or stripped of identifying details so it can no longer be linked to you.

- **Chatbot Conversation Data (End-User Data):** Data collected from end-users via your chatbot is stored on our platform until you choose to delete it or as long as your Capture AI account is active. You have control over this data through our dashboard – you can view, export, or delete conversation transcripts and leads at any time. By default, we retain chatbot interaction records to provide you the service (so you can review past chats and leads). If you delete specific data through the dashboard, it is removed from the active database. You also have the option to delete all chatbot data or specific knowledge base content you uploaded, if you no longer need it. If you require complete deletion of all data associated with your account, you may contact us to request account deletion. Upon verified request, **we will permanently delete or anonymize your personal data, including chatbot collected data, except for any information we are**

required to retain by law .

- **Logs and Analytics Data:** Usage data (such as server logs or analytics records) is typically retained for a shorter period for troubleshooting and analysis, and then either deleted or aggregated. For example, raw web server logs might be kept for a few weeks, and analytic data in Google Analytics may be retained for a set timeframe (e.g., 14 or 26 months) as configured, after which Google automatically deletes the old data.

- **Legal Compliance and Disputes:** In certain cases, we may need to retain information for longer periods if required by law (for instance, financial records for tax purposes) or to resolve disputes and enforce our agreements. If we are under a legal hold or involved in litigation, we will retain relevant data until the hold is lifted or the matter is resolved, even if that extends beyond our standard retention periods.

Once the retention period expires or the purpose of processing has been fulfilled, we will ensure the secure deletion or anonymization of the personal data. If you have any specific questions about our data retention practices (for example, where and how long your personal data is stored, or requests for erasure), you can contact us for more information .

Your Rights

You have certain rights regarding your personal information, which may vary depending on your location and the applicable privacy laws. We are committed to respecting these rights and have processes in place to enable you to exercise them.

GDPR / Data Protection Rights (EU/UK and Similar Jurisdictions)

If you are located in the United Kingdom, European Union, or other regions with similar data protection laws, you have the following rights with respect to personal data we hold about you, as provided under the GDPR and analogous laws :

- **Right to Be Informed:** You have the right to be given clear, transparent information about how we collect and use your personal data (which is the purpose of this Privacy Policy).

- **Right of Access:** You have the right to request a copy of the personal data we hold about you, and to obtain information about how we process it . This allows you to confirm whether we are processing your data and to verify its lawfulness.

- **Right to Rectification:** If any of your personal information is inaccurate or incomplete, you have the right to have it corrected or updated without undue delay.

- **Right to Erasure:** Also known as the “right to be forgotten,” this right allows you to request deletion of your personal data when it is no longer needed for the purposes for which it was collected, or when the processing is unlawful, among other reasons. We will honor valid deletion requests and will also direct any applicable service providers to delete your data, subject to any legal obligations to retain information .

- **Right to Restrict Processing:** You have the right to request that we limit the processing of your data in certain circumstances (for example, if you contest the accuracy of the data or object to our processing). While processing is restricted, we can store the data but not use it further until the issue is resolved.

- **Right to Data Portability:** You have the right to obtain your personal data in a structured, commonly used, machine-readable format and have the data transmitted to another controller where technically feasible. In practice, this means you can request us to provide your data (that you provided to us) in a CSV or similar format so that you can move it to another service .

- **Right to Object:** You have the right to object to certain types of processing, including processing based on legitimate interests and processing for direct marketing purposes. If you object, we will stop processing your personal information unless we have compelling legitimate grounds that override your rights or if needed for legal claims. Where we use your data for direct marketing, you can always object or opt-out (for example, by using the “unsubscribe” link in marketing emails).

- **Rights in Relation to Automated Decision-Making:** You have the right not to be subject to decisions based solely on automated processing (including profiling) that produce legal or similarly significant effects on you . (Note: Capture AI does not make any such automated decisions without human involvement regarding our customers. Any profiling or analytics we perform is not used to make decisions that would have a significant adverse effect on individuals.)

To exercise any of these rights, please contact us using the information in the **Contact Information** section below. We may need to verify your identity before fulfilling your request (to ensure that we don’t disclose data to an unauthorized person). We will respond to legitimate requests within the timeframe required by law (generally within one month for GDPR, with the possibility to extend by two further months if necessary). There is no fee for exercising your rights, except that we may charge a reasonable fee or refuse to act on requests that are manifestly unfounded or excessive.

Please note that some rights are subject to limitations. For example, we cannot delete data that we are required by law to keep, or we might decline a request to access data if fulfilling it would adversely affect the rights and freedoms of others. If we refuse a request, we will explain the reasons.

If you believe that our processing of your personal data infringes the law, you also have the right to lodge a complaint with a supervisory authority. In the UK, this is the Information Commissioner's Office (ICO). In the EU, you may contact the data protection authority in the country where you live or work, or where the issue occurred. We encourage you to contact us first, and we will do our best to address your concerns.

California Privacy Rights (CCPA/CPRA)

If you are a resident of California, you are protected by the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA). Even if we do not meet all thresholds that require full compliance, we strive to honor the core rights provided by these laws. Under California law, California consumers have the following rights regarding their personal information:

- **Right to Know:** You have the right to request that we disclose the specific pieces and categories of personal information we have collected about you in the past 12 months, the categories of sources of that information, the business or commercial purposes for collecting it, and the categories of third parties with whom we share it . Upon verifiable request, we will provide this information for the preceding 12 months, free of charge.

- **Right to Delete:** You have the right to request deletion of personal information we have collected from you, subject to certain exceptions . Once we receive and verify your deletion request, we will delete (and instruct our service providers to delete) your personal information from our records, unless an exception applies. For example, we may retain information needed to complete a transaction you requested, to detect security incidents, to comply with a legal obligation, or other exceptions allowed by CCPA . If we must deny a deletion request, we will explain the reason.

- **Right to Correct:** (Effective January 1, 2023, under CPRA) You have the right to request correction of inaccurate personal information that we maintain about you. Upon verification, we will correct the information as you direct, taking into account the nature of the personal information and purposes of processing.

- **Right to Opt-Out of Sale or Sharing:** You have the right to opt-out of the "sale" or "sharing" of your personal information. However, *please note: Capture AI does not sell personal information to third parties for monetary or other valuable consideration* . We also do not share your personal information with third parties for cross-context behavioral advertising (as defined under the CPRA). Because we do not sell or share personal data in this way, we do not offer a "Do Not Sell or Share My Personal Information" link at this time. If this changes, we will update our policy and provide a mechanism for opt-out.

- **Right to Non-Discrimination:** We will not discriminate against you for exercising any of your CCPA rights. This means we will not deny you services, charge you a different

price, or provide a different level or quality of service just because you exercised your privacy rights. However, please understand that deleting your data may affect our ability to provide certain services you requested (for example, if you ask us to delete all of your data, we cannot provide services that rely on that data).

To exercise your California privacy rights, you (or your authorized representative) can submit a verifiable request to us – see **Contact Information** below for how to reach us . Your request should include sufficient information that allows us to verify you are the person about whom we collected personal information (or an authorized agent for that person), and it should describe your request with enough detail so we can properly understand and respond . We will take steps to verify your identity using information we have (for instance, by confirming control of your email address or other information). You may also be required to confirm that you are a California resident. We aim to respond to requests within 45 days as required by CCPA (with an extension of another 45 days if needed, with notification to you).

If you have an authorized agent making a request on your behalf, we may require proof of the agent's registration with the California Secretary of State (if the agent is a business) or a valid power of attorney or a written authorization signed by you. We will also verify the identity of the agent.

For clarity, in the past 12 months, we have **not sold any personal information** and have only disclosed personal information for business purposes consistent with this policy (such as providing data to our service providers). We do not knowingly collect or sell the personal information of minors under 16 years of age without affirmative authorization.

Other US State Privacy Rights

If you are a resident of certain other states (such as Virginia, Colorado, Connecticut, or Utah) that have enacted their own privacy laws, you may have similar rights to access, correct, delete, or opt-out of certain data processing. Capture AI will honor valid requests from residents of these states in line with the applicable law. For example, if you are a Virginia resident, you have the right to confirm whether we process your personal data and to access, correct, delete, or obtain a copy of your data, as well as to opt-out of targeted advertising or any sale of data (which, as noted, we do not do). To exercise any rights, please contact us and we will facilitate your request in accordance with applicable law.

We will not charge a fee for handling your request unless it is excessive, repetitive, or manifestly unfounded, in which case we may charge a reasonable fee or refuse to act on the request as permitted by law.

Cookies and Tracking Technologies

Cookies are small text files that websites store on your device to remember information about you, such as your preferences or login status. We, and our third-party partners, use cookies and

similar tracking technologies (such as web beacons, pixels, and local storage) to collect information automatically when you use our website and services. This section explains how we use these technologies and what choices you have.

Types of Cookies We Use:

- **Essential Cookies:** These cookies are necessary for our website and dashboard to function properly. For example, they help authenticate your login and keep your session active, or enable you to move around the site and use its features. Without these cookies, certain services you have asked for (like accessing secure account areas) cannot be provided. These cookies do not gather information for marketing but are purely technical. Because they are necessary, you cannot opt-out of essential cookies via our cookie banner (if present), though you can still block them using browser settings (but this may impair site functionality).

- **Analytics Cookies:** We use analytics or performance cookies to understand how visitors engage with our website. For instance, **Google Analytics** cookies allow us to collect information about website usage, such as which pages users visit, how long they stay, and any errors encountered. The data collected is aggregated and helps us improve the website's user experience and performance. Google Analytics may set cookies such as _ga and _gid to distinguish users and throttle request rates. The information obtained through analytics cookies is subject to Google's Privacy Policy . We have configured Google Analytics in a privacy-conscious manner (e.g., IP anonymization is enabled, where available, to truncate your IP address). We do not use analytics cookies to identify you personally; they are used for statistical purposes.

- **Advertising and Tracking Cookies:** We may use advertising cookies or pixels from services like Facebook, Google Ads, or others to help with our marketing initiatives. For example, the **Facebook Pixel** on our site tracks when a user takes certain actions (like visiting a specific page) after clicking on our Facebook ads. This helps us measure ad conversions and effectiveness. The data collected (such as device ID or pixel ID and the event performed) is sent to the respective platform. We use it to create reports on ad performance and to improve our ads – for example, the Facebook Pixel allows us to know which ad campaigns are successful for **statistical and market research purposes** . We do *not* use these cookies to profile you for third-party advertising, nor do we share or sell this data to outside advertisers. If we engage in any re-targeting ads (showing our ads to you on other sites after you visited our site), these cookies would facilitate that, but such activity would only be for promoting Capture AI's own services. Advertising platforms might use the data collected via their cookies for their own purposes; please refer to the privacy policies of those platforms (e.g., Facebook's Data Policy, Google's Privacy Policy) for more details.

- **Functionality Cookies:** These cookies allow our site to remember choices you make (such as your language or region) and provide enhanced features. For instance, if we have a cookie consent banner, once you choose your cookie preferences, a cookie will

remember that selection so you don't have to re-enter it. Similarly, if our application has a feature tour that you dismiss, a cookie might remember that so it doesn't show again.

We may also use **local storage** or similar technologies in our web application to remember your preferences or the state of the interface (for example, storing user settings or caching content for performance). These operate similarly to cookies in terms of your ability to control them.

Your Choices and Controls:

When you first visit our site, you may be presented with a cookie notice or banner that allows you to accept or manage non-essential cookies. You can always change your cookie preferences by adjusting your browser settings. Most web browsers allow you to refuse or delete cookies – for example, by activating the setting on your browser that allows you to refuse all or some cookies. You can also delete cookies that have already been set. Please note that if you disable or delete cookies, some parts of our site (especially the logged-in dashboard or chatbot functionality) might not function properly, because essential cookies may be required for those features.

For analytics cookies, Google provides an opt-out mechanism: you can install the Google Analytics Opt-out Browser Add-on which prevents Google Analytics from collecting information on your visits to our site (this works in supported browsers). For interest-based advertising, you can manage your preferences through industry websites such as the Network Advertising Initiative Opt-Out page or the DAA's WebChoices Tool. If you opt out via these tools, an "opt-out cookie" will be placed on your browser indicating your choice; if you clear cookies, you may need to opt-out again.

Additionally, for the Facebook Pixel, you can adjust your ad settings in your Facebook user account to control whether you see targeted ads (see Facebook's **Opt-Out** instructions). For Google Ads, you can visit Google Ads Settings to manage your preferences or opt out of personalized ads .

Keep in mind that declining certain cookies may affect your experience. For example, if you block all cookies, you may need to re-enter preferences every time, and some features might not work. But we provide these choices to give you control over your data.

For more information on cookies and how to manage them, you can also visit **allaboutcookies.org** (a useful resource with instructions for different browsers) .

Third-Party Services

As described above, Capture AI relies on a number of third-party services to operate our platform. We want to be transparent about these third parties and how they handle data:

- **Stripe (Payment Processing):** Stripe Inc. is our payment processor for handling subscription payments. When you enter payment information, it is sent directly to Stripe via embedded secure forms. Stripe will process your payment data under its strict security protocols (including PCI-DSS compliance) and will store your payment card tokens or identifiers on our behalf. We do not have access to your full credit card details – we may only see information like the last four digits of your card, card type, and expiration date for reference. Stripe may also collect some personal information about you (such as your name, email, billing address, and transaction amount) to process the payment and for fraud prevention. Stripe **will not use your personal information for any purpose other than providing payment services to us**, as per their privacy policy. For more information, you can refer to Stripe's Privacy Policy . By using our paid services, you acknowledge that your payment information will be processed by Stripe, which is a separate data controller for that information.

- **Google Analytics (Website Analytics):** As noted, we use Google Analytics provided by Google LLC. Google Analytics uses cookies and similar technologies to collect data about visitors (e.g., IP address, device info, site behavior). Google acts as a data processor for us, meaning it processes the data only on our instructions. However, Google may use some data for its own analytics purposes; we have disabled data sharing with Google where feasible and do not use other Google Analytics features that would allow Google to use our data for advertising (such as remarketing audiences or integrating with Google AdSense). The information generated by Google Analytics cookies about your use of our site is generally transmitted to and stored by Google on servers in the United States. Google is certified under frameworks like the EU-U.S. Data Privacy Framework (as of the latest update) or relies on Standard Contractual Clauses for international transfers. You can learn more about Google's data practices in the Google Analytics Help or Google's Privacy Policy . If you prefer not to be included in Google Analytics data, please use the opt-out methods described above (browser add-on or cookie settings).

- **Voiceflow (Chat Widget Provider):** Voiceflow, Inc. provides the chat widget and conversational engine technology that we leverage for deploying chatbots on your site. When an end-user interacts with the chatbot, their messages and inputs are handled by Voiceflow's systems, which then work with our platform's knowledge base to generate responses. In essence, Voiceflow is a sub-processor for any personal data (like chat content or user-provided contact info) that flows through the chatbot widget. We have a Data Processing Agreement in place with Voiceflow to ensure they protect the data in compliance with GDPR and other laws. According to Voiceflow's privacy commitments, they do not access or use the content of conversations except as necessary to deliver the service (for example, temporarily processing the text to route the conversation) . Voiceflow does not keep or use your chatbot data to train their models or for any marketing purposes. They may collect some technical information (like IP address or usage logs) about the operation of the widget, to monitor uptime and performance. All such data is handled under their privacy policy and remains under our control as per our

agreement. If you would like to review Voiceflow's privacy practices, you can find their Privacy Policy on their website. In summary, using our chatbot involves sending end-user queries and your configured content to Voiceflow's platform, but this data remains confidential and is not shared further.

- **Cloud Hosting (e.g., Amazon Web Services/Azure/Google Cloud):** We host Capture AI on reputable cloud infrastructure. Our databases, application servers, and file storage may reside on these platforms. These cloud providers act as **infrastructure providers** and *sub-processors*. They might physically store or transmit personal data, but they do not access it except for maintaining and running our environment. We configure our systems with high security; for example, data at rest on cloud storage is encrypted and access is restricted to our operations team. Cloud providers have their own compliance certifications (like ISO 27001, SOC 2, etc.) which ensure a high level of security. If data is stored outside your country (for instance, on US servers), we address that under **International Data Transfers** below with appropriate safeguards .

- **Email and Communication Tools:** We may use third-party email services (for example, an email sending service or support ticketing system) to send transactional emails (like welcome emails, password resets, or notifications) and to manage support queries. These providers will process your contact information and message content as needed to fulfill their function. We ensure any such providers are GDPR-compliant and offer sufficient guarantees of security. They will not use your information for their own purposes.

- **Advertising Partners:** If we run marketing campaigns, we might use platforms like Google Ads, Facebook/Meta, LinkedIn, etc. to reach new customers. While we do not share your personal data directly with these platforms except as needed (e.g., we might upload a list of business emails for a custom audience, but only in compliance with law and with opt-out options), these platforms might collect data via cookies or pixels on our site as described earlier. We contractually and through platform settings limit any data use to what is needed for our campaign performance. For example, we have agreed to Meta's Business Tools Terms which limit how data collected via the Facebook Pixel can be used – the data is provided to us in aggregated form for analytics and can only be used by us internally . We do not allow these ad partners to collect sensitive information or to use the data for purposes outside our instructions.

Each of these third-party services has its own privacy policy. While we carefully choose our partners and strive to include only those with strong privacy and security standards, we encourage you to review their privacy notices to understand how they handle your data. Where required by law, we have entered into Data Processing Addendums (DPAs) with these providers to ensure they only process personal data under our instructions and in compliance with GDPR or other applicable laws.

If you have questions about any specific third-party integration or service, please contact us. We can provide more details on what data is shared and how it is protected in the context of that service.

Children's Privacy

Our website and services are **not directed to children**, and we do not knowingly collect personal information from individuals under the age of 13 (or under the relevant age of consent in your jurisdiction, if higher). Capture AI is intended for use by businesses and adults; children should not use our platform or chatbot services.

We do not knowingly solicit or receive information from children . In fact, our terms of service require that users be at least 18 years of age (or the age of majority in their location) to create an account. We also advise our customers that their chatbot implementations should not target children under 13 or collect information from such children without parental consent, to comply with laws like COPPA.

If you are under 13, please do not submit any personal information to us, use our chatbots, or sign up on our site. If we become aware that we have inadvertently collected personal data from a child under 13 (for example, if a child sends personal details in a chatbot conversation without our knowledge), **we will promptly take steps to delete that information from our records** . If a parent or guardian discovers that a child has provided us with personal information, they should contact us, and we will delete the information.

For minors aged 13 to 16 in California, we also do not sell any personal information (and would not do so even with opt-in, as per our no-sale policy). If in the future we were to engage in any practice that involved personal data of minors, we would comply with all applicable laws and obtain proper consent.

If you have any concerns about children's privacy related to our services, please contact us using the details below. We encourage parents and legal guardians to monitor their children's internet usage and to help enforce this Privacy Policy by instructing minors to never provide personal data through our services.

International Data Transfers

Capture AI is based in the United Kingdom, but we serve customers around the world. The data we collect from you may be transferred to, stored in, and processed in countries other than your own, including the United States and other locations where our service providers operate. **This means your personal information may be transferred to jurisdictions that may not have the same data protection laws as your home country.**

If you are located in the UK, European Union, or European Economic Area (EEA), we will ensure that adequate safeguards are in place for any transfer of personal data outside of the

UK/EEA. Specifically, when we transfer EU/UK personal data to the United States or other countries not deemed “adequate” by the European Commission or UK authorities, we rely on appropriate transfer mechanisms such as the European Commission’s **Standard Contractual Clauses (SCCs)** (as permitted under GDPR Article 46) . These are contractual commitments between us and the recipient of the data (e.g., our US-based service providers) that require them to protect personal data according to GDPR standards. In some cases, we may also rely on an applicable **adequacy decision** (if the country has been approved by the EU/UK as having essentially equivalent protection) or other derogations where allowed (such as your explicit consent or necessity for contract fulfillment, in limited situations).

We have assessed our key service providers for their data transfer practices. For example, Google and Stripe are participants in data transfer frameworks or implement SCCs. Voiceflow, as a Canada-based company, benefits from the EU’s adequacy decision for Canada for certain data (personal data processed by Canadian organizations subject to Canadian law is considered protected). For any processing of EU data in the US by Voiceflow or others, SCCs are in place as needed . We also take into account any supplementary measures recommended by regulators (like encryption in transit and at rest, minimization of data sent, etc.) to ensure transferred data remains protected.

We want to be transparent: **the United States (where some of our data may reside) does not have an adequacy decision from the EU**, meaning its privacy laws are considered not equivalent in all respects . However, by implementing the safeguards mentioned and reviewing our partners’ security measures, we endeavor to provide an adequate level of protection for your data in line with EU/UK requirements . We also monitor legal developments (such as new transfer frameworks or guidance from data protection authorities) and will adapt our practices accordingly.

If you would like more information about our data transfer practices or need a copy of the relevant SCCs, you can contact us (see **Contact Information** below) . We will be happy to discuss how your data is protected or provide relevant documentation subject to confidentiality.

By using our website or services, or by providing us with your information, you **consent to the transfer of your personal data across international borders** as described here (to the extent such consent is required and valid under your local law). We will of course handle that personal data in accordance with this Privacy Policy and applicable law no matter where it is processed.

Changes to This Privacy Policy

We may update or revise this Privacy Policy from time to time to reflect changes in our practices, technologies, legal requirements, or for other operational reasons . When we make changes, we will post the updated policy on this page and update the “Last Updated” date at the top of the policy. If the changes are significant, we will provide a more prominent notice (such as on our homepage or via email notification to account holders) to inform you of the update.

Any updated version of the Privacy Policy will be effective as soon as it is posted, unless otherwise specified. In certain cases, if required by law, we may seek your explicit consent to material changes in how we use your data.

We encourage you to review this Privacy Policy periodically to stay informed about our data practices. **Your continued use of Capture AI after any changes to this Privacy Policy constitutes your acceptance of the revised policy**, to the extent permitted by law . If you do not agree with the changes, you should discontinue use of our services and contact us regarding deletion of your data.

Contact Information

If you have any questions, concerns, or requests regarding this Privacy Policy or our handling of your personal information, please contact us:

High Jump Digital Limited (Capture AI)

71-75 Shelton Street, Covent Garden

London, WC2H 9JQ

United Kingdom

Email: support@cptr.ai

We will do our best to respond promptly to your inquiry. If you are contacting us to exercise a privacy right, please include sufficient detail so we can properly understand and respond to your request (and if applicable, verify your identity).

If you feel we have not addressed your privacy-related concern adequately, you may have the right to contact your local data protection authority (such as the ICO in the UK or a EU supervisory authority, or your state Attorney General's office in the U.S.) to file a complaint.

Thank you for entrusting Capture AI with your data. We are committed to protecting your privacy and using your information responsibly.