

## **Inkeep, Inc.**

### **Privacy Policy**

Last updated: October 2, 2023

At Inkeep, Inc. (“**Inkeep**,” “**we**,” “**us**”) we consider the privacy and the security of personal data to be extremely important.

We process personal data in connection with the use of Inkeep’s website, services, software, mobile applications, content, AI Functions and all other products and services (all of the foregoing collectively, the “**Services**”).

In this Privacy Policy, we describe how we process personal data of the following data subjects:

- our customers, their end users and representatives,
- website users,
- email or newsletter subscribers,
- potential customers.

This Privacy Policy covers information collected through the Services, on our website [www.inkeep.com](http://www.inkeep.com) or other websites administered by Inkeep where the Privacy Policy is placed (the “**Site**”) and in other sources.

The Privacy Policy is incorporated by reference into our Terms of Service, currently available at <https://inkeep.com/policies/terms-of-service> (the “**Terms of Service**”). Any terms used herein and not defined will have the meanings given to them in the Terms of Service. By using the Services, you hereby warrant and represent that you have read, understand and agree to this Privacy Policy and the Terms of Service and that you are over 18 years of age. PLEASE DO NOT USE, INSTALL OR ACCESS THE SERVICES IF YOU DO NOT AGREE TO THIS PRIVACY POLICY.

We have no direct relationship with your end users or any person other than you, and for that reason, you are responsible for making sure that your end users and any other representatives comply with this Privacy Policy and that you have the appropriate permission and legal basis for us to collect and process information about those individuals.

If you have any questions or suggestions concerning our privacy practices, please email us at [privacy@inkeep.com](mailto:privacy@inkeep.com). Please also send us an email if you would like to request data access or deletion, or to exercise other rights as a data subject.

#### **1. How We Collect Personal Data**

What personal data we collect depends largely on the interaction that takes place between you and Inkeep, most of which can be categorized under the following:

- **When you use Inkeep’s Services.** When you or your end users use Inkeep’s Services, we store all User Content that you or your end users provide for use with the AI Functions or when using the

AI Functions, account details and other personal data provided by you or your end users, including content from third party integrations that you choose to link to the Services. We gather this information from you or your end users directly when provided or entered by you or your end users, or from integrations linked to the Services.

In some cases, we can receive information from third parties, e.g. from a payment service provider on whether your payment was successful.

- **When you send us emails or message us.** When we receive emails or messages from you or your end users, we can store the content of such emails, including attachments as well as your or your end user's contact details.
- **When you submit forms on the Site.** When you complete forms on the Site (contact us, subscription, demo request, etc.) we collect your contact details and information you complete in the form.
- **When you use the Site.** When you use the Site, we collect certain information, as described in more detail below that may, alone or in combination with other information, constitute personal data (e.g. cookie files).

## 2. What Types of Personal Data We Process

### *Information You Provide To Us*

We collect and process the following personal data that you or your end users provide to us:

- **Customer account details.** To create or update your account and provide the Services we collect from you and third-party integrations information about you and your end users. This includes name, email, phone number, products in use, location, and any other information you decide to provide.
- **Personal data within User Content.** As you use our Services, you may include in User Content that is uploaded or provided for use with the AI Functions personal data you have collected from your users, employees customers, prospective customers or other individuals. We process this data only on your behalf as our customer. We have no direct relationship with any person other than you, and for that reason, you are responsible for making sure you have the appropriate permission and legal basis for us to collect and process information about those individuals.
- **Financial information.** To process your payments for the Services subscription, we need your credit card details (last four digits of the card number), account details and payment information.
- **Contact details and business data.** We receive information about our customers and potential customers for cooperation and communication purposes. This includes full name, title, company, email or other contact details as may be necessary.
- **Requests, messages and submitted forms details.** We receive and process your or your end users messages, support requests, emails and information you share with us via online forms, online forums, social media accounts or other support channels. This includes the content of such communications as well as your contact details if any.

We ask that you not provide or disclose to us any sensitive personal data (e.g., social security numbers, information related to racial or ethnic origin, political opinions, religion or other beliefs, health, biometrics or genetic characteristics, criminal background or union membership) on or through the

Services or otherwise. You are responsible for making sure that your end users do not provide or disclose to us any sensitive personal data on or through the Services, within any User Content or otherwise.

### ***Automatically Collected Information***

Most of the data we collect in and through the Site and the Services is technical in nature and is collected and processed automatically through so-called application programming interfaces, software development kits, cookies and similar software-based technologies. Alone or in combination with other data, such automatically collected data may constitute personal data. The data we may collect by automated means may include, without limitation:

- Device data: including, but not limited to, data on device ID's and similar hardware qualifiers, and precise location data.
- Usage data: including, but not limited to, search terms entered and pages viewed.
- Network and internet information: including, but not limited to, URLs, Internet Protocol addresses, bounce rates, use of spoofing, active (TCP/IP) ports, number of sessions initiated, click streams, location information and network/Wi-Fi access points.
- Information we collect on the use of the Site via cookies: please see the "How We Use Cookies and Other Technologies" section below for more information.

We may use, depending on the Services, (i) location based on the IP address presented by you or your end users, (ii) network-based geo-location data based on proximity of network towers or the location of Wi-Fi networks, and/or (iii) geo-location data based on coordinates obtained from a mobile device's GPS radio and location services. Your or your end users' GPS geo-location is accessed in accordance with device settings. If location services are enabled on your or your end users' mobile device and/or a mobile application in connection with the Services, certain of the Services will passively and automatically send location information to Inkeep in order to for us to deliver location-specific information on such device and compile your or your end users' individualized timeline. Please note that disabling location service will not anonymize data already collected and uploaded to our servers.

### ***Information You Share on Third Party Websites or through Social Media Services***

The Services may include links to third party websites and social media services where you will be able to post comments, stories, reviews or other information. Your use of these third party websites and social media services may result in the collection or sharing of information about you by these third party websites and social media services. We encourage you to review the privacy policies and settings on the third party websites and social media services with which you interact to make sure you understand the information that may be collected, used, and shared by those third party websites and social media services.

## **3. For Which Purposes We Use Personal Data**

We collect and process your or your end users' personal data for the following purposes:

- **To operate the Services:** We use personal data to enter into the agreement with you as a customer and operate, maintain and administer your account in the Services, as well as to communicate with you regarding the account (sending announcements, technical notices, updates, security alerts, and support and administrative messages) and to respond to Service-related requests, questions and feedback. We also use your data to perform our billing obligations. To the extent any User Content contains personal data, we may process this data on your behalf to provide the Services.
- **To improve our Services:** We process your and your end users’ personal data to understand how you use our Services and Site, including to monitor usage or traffic patterns and to analyze trends and develop new products, services, features and functionality in reliance on our legitimate interests and to train, develop, improve and optimize the AI Functions and our Services and Site. WE DO NOT USE YOUR PERSONAL DATA TO TRAIN ANY LARGE LANGUAGE MODELS OR OTHER FOUNDATIONAL MODELS WHERE YOUR PERSONAL DATA COULD BE EXPOSED TO THIRD PARTIES.
- **To communicate with you and inform you about the Services.** If you request information from us, register for the Services, complete a form or feedback on a Site, or participate in our surveys, we may send you Inkeep-related marketing communications if permitted by law. In all such communications, we will provide you with the possibility to opt-out.
- **To comply with law.** We use your or your end users’ personal data as necessary to comply with applicable laws, including sanction requirements, accounting and tax obligations, legal processes or audits, to respond to subpoenas or legally binding requests from government authorities. Before disclosing any information to an authority upon its request, we check the validity of such request carefully.
- **For compliance and safety.** We use your or your end users’ personal data as we believe necessary or appropriate to (a) enforce the terms and conditions that govern the Services; (b) protect our rights, privacy, safety or property, and/or that of you or others; and (c) protect, investigate and deter against fraudulent, harmful, unauthorized, unethical or illegal activity.

#### 4. How We Use Cookies and Other Technologies

Some of the features on the Site and the Services require the use of “cookies” - small text files that are stored on your or your end users’ device’s hard drive. We use cookies to measure which pages are being accessed, and which features are most frequently used. This enables us to continuously improve the Site and Services to meet the needs of our visitors.

The following sets out how we may use different categories of cookies and your options for managing cookie settings:

Type of Cookies	Description	Managing Settings
<b>Required cookies</b>	Required cookies enable you and your end users to navigate the Site and use their features, such as accessing secure areas of the Site and using the Services. If you or your end users have chosen to identify yourself to us, we use cookies containing encrypted information to allow us to uniquely identify you or your end	Because required cookies are essential to operate the Site and the Services, there is no option to opt out of these cookies.

	user. These cookies allow us to uniquely identify you or your end user when logged into the Site and to process online transactions and requests.	
<b>Performance cookies</b>	These cookies collect information about how you or your end users use our Sites, including which pages you or they go to most often and if you or they receive error messages from certain pages. These cookies do not collect information that individually identifies you or your end users. Information is only used to improve how the Site functions and performs. From time-to-time, we may engage third parties to track and analyze usage and volume statistical information relating to individuals who visit the Site or use the Services. We may also utilize Flash cookies for these purposes.	To learn how to opt out of performance cookies using browser settings, <a href="#">click here</a> . To learn how to manage privacy and storage settings for Flash cookies, <a href="#">click here</a> .
<b>Functionality cookies</b>	Functionality cookies allow our Sites to remember information you or your end users have entered or choices you or your end users make (such as username, language, or your region) and provide enhanced, more personal features. These cookies also enable you or your end users to optimize your use of the Site after logging in. These cookies can also be used to remember changes made to text size, fonts and other parts of web pages that are customizable. We may use local shared objects, also known as Flash cookies, to store preferences or display content based upon what you or your end users view on the Site to personalize your or their visit.	To learn how to opt out of functionality cookies using browser settings, <a href="#">click here</a> . To learn how to manage privacy and storage settings for Flash cookies, <a href="#">click here</a> .

We and our service providers may also use “pixel tags,” “web beacons,” “clear GIFs,” or similar means in connection with the Services and HTML-formatted email messages to, among other things, track the actions of users, to determine the success of marketing campaigns and to compile aggregate statistics about Site or Service usage and response rates.

## 5. How We Share Personal Data

We do not sell your data or your end users’ data to third parties for commercial or advertising purposes. We share your data and your end users’ data as described in this Privacy Policy or upon obtaining your consent for such data sharing.

We disclose personal data to third parties under the following circumstances:

- **Service Providers.** We employ third-party companies and individuals to help us with performance of certain activities, e.g. payment service providers. We also use third-party software to process data (e.g. CRM, email agent, cloud storage solutions, etc.).

We also use third-party cookies on the Site.

These third parties are permitted to use personal data about you or your end users only to perform these tasks for lawful business purposes in accordance with the terms of the agreement(s) we have in place with such service providers and for no other purpose.

- **Professional Advisors.** We may disclose your or your end users' personal data to professional advisors, such as lawyers, bankers, auditors and insurers, where necessary in the course of the professional services that they render to us.
- **Third-party Applications and Integrations.** For the provision of the Services we may receive and share data with third-party integrations and apps that you choose to link to the Services. We may attempt to de-identify or anonymize personal data that is received or shared with third party integrations and apps, but we cannot guarantee that any personal data received from or shared with third party integrations and apps is de-identified or anonymized.
- **Business Transfers.** As we develop our business, we might sell or buy businesses or assets. In the event of a corporate sale, merger, reorganization, dissolution or similar event, personal data may be part of the transferred assets. You acknowledge and agree that any successor to or acquirer of Inkeep (or its assets) will continue to have the right to use your and your end users' personal data and other information in accordance with the terms of this Privacy Policy. Further, Inkeep may also disclose aggregated personal data in order to describe our Services to prospective acquirers or business partners.
- **Compliance with Laws and Law Enforcement.** Inkeep may disclose information about you or your end users to government or law enforcement officials or private parties as required by law, and disclose and use such information as we believe necessary or appropriate to (a) comply with applicable laws and lawful requests and legal processes, such as to respond to subpoenas or requests from government authorities; (b) enforce the terms and conditions that govern the Services; (d) protect our rights, privacy, safety or property, and/or that of you or others; and (e) protect, investigate and deter against fraudulent, harmful, unauthorized, unethical or illegal activity.
- **Corporate Affiliates.** We may share personal data with our corporate affiliates.

## 6. Your Data Protection Rights & Choices

You have the following rights:

- If you wish to **access** your personal data that Inkeep collects, you can do so at any time by contacting us.
- You can also contact us to **update, correct or delete** information in your account.
- If you are in the European Economic Area (“**EEA**”), the UK, or Switzerland, you can **object to processing** of your personal data, ask us to **restrict processing** of your personal data or **request portability** of your personal data where it is technically possible.

- Similarly, if you are in the EEA, the UK, or Switzerland, and provided we have collected and processed your personal data under your consent, then you can **withdraw your consent** at any time. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your personal data conducted in reliance on other lawful processing grounds.
- You have the **right to complain to a data protection authority** about our collection and use of your personal data. Contact details for data protection authorities in the EEA, Switzerland and certain non-European countries (including the U.S. and Canada) are available [here](#).

You may submit your request via <https://inkeep.com/privacy/data-request> or by sending an email to [privacy@inkeep.com](mailto:privacy@inkeep.com). We will respond to all requests in accordance with applicable data protection laws.

**Access to Data Controlled by our Customers.** We don't have any direct relationships with customers' end users. An individual end user who seeks access, or who seeks to correct, amend, or delete personal data processed in the Services by our customers should direct their request to the customer directly.

## 7. Data Transfers

Your personal data may be stored and processed in any country where we have facilities or in which we engage service providers, including in the U.S.

By accepting the terms of this Privacy Policy, you acknowledge and agree to (1) the transfer to and processing of personal data on servers located outside of the country where you reside and (2) our collection and use of your or your end users' personal data as described herein and in accordance with the data protection laws of the countries in which we have facilities or in which we engage service providers, which may be different and may be less protective than those in your country.

## 8. Personal Data Transferred from the EA, the UK or Switzerland to the United States

Inkeep operates in countries outside the EEA, the UK, and Switzerland, such as the U.S., and may utilize data processors and sub-processors located in third countries.

If you are located in the EEA, the UK, or Switzerland, this means that we may transfer personal data outside of your country. Such transfers are made using appropriate safeguards and supplementary measures. We enter into the EU Standard Contractual Clauses for data transfers with our customers who use the Services.

## 9. Children's Information

We believe it is important to provide added protection for children online. We encourage parents and guardians to spend time online with their children to observe, participate in and/or monitor, and guide their online activity. The Site and/or the Services are not intended for use by anyone under the age of 18, nor does Inkeep knowingly collect or solicit personal data from anyone under the age of 18.

If you are under 18, you may not attempt to register for the Services or send any information about yourself to us, including your name, address, telephone number, or email address. In the event that we confirm that we have collected personal data from someone under the age of 18 without verification of parental consent, we will delete that information promptly. If you are a parent or legal guardian of a child under 18 and believe that we might have any information from or about such a child, please contact us. We do not sell any personal data of our customers, including those aged between 13 to 18.

## **10. Security**

### **Safeguarding Your Information**

We take reasonable and appropriate measures to protect personal data from loss, misuse and unauthorized access, disclosure, alteration, and destruction, taking into account the risks involved in the processing and the nature of the personal data.

Despite these efforts to store personal data collected on and through the Site and/or the Services and otherwise by us in a secure operating environment that is not available to the public, we cannot guarantee the security of personal data during its transmission or its storage in our systems. Further, while we attempt to ensure the integrity and security of personal data, we cannot guarantee that our security measures will prevent third-parties such as so-called hackers from illegally obtaining access to personal data. We do not warrant or represent that personal data about you will be protected against, loss, misuse, or alteration by third parties.

The credit card processing vendor we work with uses security measures to protect your information both during the transaction and after it is complete.

If you have any questions about the security of your personal data, you may contact us by email [privacy@inkeep.com](mailto:privacy@inkeep.com).

### **Notice of Breach of Security**

If a security breach causes an unauthorized intrusion into our system that materially affects you or your end users, then we will notify you as soon as possible and later report the action we took in response.

## **11. Legal Basis for Processing Your Personal Data (EEA Visitors/Customers Only)**

If you are a person located in the EEA or the UK our legal basis for collecting and using the personal data described above will depend on the purpose of processing and personal data concerned:

- We process data to perform a contract with you on use of the Services (Art. 6(1)(b) of the GDPR or UK GDPR);
- We also process data based on our legitimate interest (Art. 6(1)(f) of the GDPR or UK GDPR) in the following cases:
  - to communicate with you and inform about our Services;
  - to comply with the law we are subject to;
  - to conduct events and communicate with you;
  - to negotiate, enter and perform agreements;



- for compliance and safety.
- We process some types of cookie files based on your consent (Art. 6(1)(a) of the GDPR or UK GDPR).

If we ask you to provide personal data to comply with a legal requirement or to enter into a contract with you, we will make this clear at the relevant time and advise you whether the provision of your personal data is mandatory or not (as well as of the possible consequences if you do not provide your personal data). Similarly, if we collect and use your personal data in reliance on our legitimate business interests, we will make clear to you at the relevant time what those legitimate business interests are.

You are not obliged to provide your personal data to us. However, if we need personal data in order to enter and perform the contract with you and you do not provide this data, we may not be able to perform the contract we have or are trying to enter into with you.

If you have questions about or need further information concerning the legal basis on which we collect and use your personal data, you may contact us by email at [privacy@inkeep.com](mailto:privacy@inkeep.com).

## **12. For California Residents**

If you are a resident of California, California Civil Code Section 1798.83 permits you to request information regarding how we disclosed your personal data to third parties for such parties' direct marketing purposes during the preceding calendar year. To request the above information, please contact us at [privacy@inkeep.com](mailto:privacy@inkeep.com). We will respond to such requests for information access within 30 days following receipt at the e-mail or mailing address stated below. Please note that we are only required to respond to an individual once per calendar year.

Besides, California Data Protection Laws (California Consumer Privacy Act of 2018 and the California Privacy Rights Act of 2020, as each may be amended or replaced from time to time) give you the following specific rights as a California resident:

### **1. Requests to Know**

You have the right to request that we disclose:

- The categories of personal data we have collected about you;
- The categories of personal data about you we have sold or disclosed for a business purpose;
- The categories of sources from which we have collected personal data about you;
- The business or commercial purposes for selling, sharing or collecting personal data about you;
- The categories of personal data sold or shared, if any, about you, as well as the categories of third parties to whom the personal data was disclosed, by category of personal data for each party to whom personal data was sold; and
- The specific pieces of personal data collected.

You may submit a request to know via <https://inkeep.com/privacy/data-request> or contacting us at [privacy@inkeep.com](mailto:privacy@inkeep.com). The delivery of our response may take place electronically or by mail. We are not required to respond to requests to know more than twice in a 12-month period.

We do not sell, and have not in the prior 12 months sold, Personal Information (as defined in the California Data Protection Laws) about California residents. Therefore, we have not included a “Do Not Sell My Personal Info” link on our Site. If our practices change, we will update this Privacy Policy and take any other necessary action to comply with applicable law. We do, however, disclose Personal Information for business purposes as described in the “How We Share Personal Data” section above.

## **2. Requests to Delete**

You have the right to request that we delete any personal data about you that we have collected. Upon receiving a verified request to delete personal data, we will do so unless otherwise required or authorized by law. You may submit a request to delete personal data via <https://inkeep.com/privacy/data-request> or contacting us at [privacy@inkeep.com](mailto:privacy@inkeep.com).

## **3. Authorized Agents**

You may designate an authorized agent to make requests on your behalf. You must provide an authorized agent written permission to submit a request on your behalf, and we may require that you verify your identity directly with us and confirm with us that you provided the authorized agent permission to submit the rights request. This verification process is not necessary if your authorized agent provides documentation reflecting that the authorized agent has the power of attorney to act on your behalf under Cal. Prob. Code §§ 4121 to 4130.

## **4. Methods for Submitting Consumer Requests and Our Response to Requests**

You may submit a request for access and requests to delete personal data about you via: <https://inkeep.com/privacy/data-request> or contacting us at [privacy@inkeep.com](mailto:privacy@inkeep.com)

Upon receipt of a request, we may ask you for additional information to verify your identity. Any additional information you provide will be used only to verify your identity and not for any other purpose.

We will acknowledge the receipt of your request within ten (10) business days of receipt. Subject to our ability to verify your identity, we will respond to your request within 45 calendar days of receipt. If we require more time (up to 90 days), we will inform you of the reason and extension period in writing. In order to protect your privacy and the security of personal data about you, we verify your request by email.

Any disclosures we provide will only cover the 12-month period preceding the verifiable consumer request's receipt. The response we provide will also explain the reasons we cannot comply with a request, if applicable.

We do not charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

We do not currently alter our practices when a Do Not Track signal is received, because at this time no formal “Do Not Track” standard has been adopted. To learn about Do Not Track and for information about how to opt-out of receiving targeted advertising, please click [www.aboutads.info/choices](http://www.aboutads.info/choices).

## **5. The Right to Non-Discrimination**

You have the right not to be discriminated against for the exercise of your California privacy rights described above. Unless permitted by the California Consumer Privacy Act, we will not:

- Deny you goods or services.
- Charge you different prices or rates for goods or services, including through granting discounts or other benefits, or imposing penalties.
- Provide you with a different level or quality of goods or services.
- Suggest that you may receive a different price or rate for goods or services or a different level or quality of goods or services.

## **13. Data Retention**

We keep personal data related to your Account for as long as it is needed to fulfill the purposes for which it was collected, to provide our services, to deal with possible legal claims, to comply with our business interests and/or to abide by all applicable laws. Thereafter, we either delete personal data about you or de-identify it. Please note that even if you request the deletion of personal data about you, we may be required (by law or otherwise) to retain the personal data and not delete it. However, once those requirements are removed, we will delete personal data about you in accordance with your request.

## **14. Changes to Our Privacy Policy**

We may need to change this Privacy Policy from time to time to reflect legal, technical or business developments. When we update our Privacy Policy, we will take appropriate measures to inform you before its entry into force, consistent with the significance of the changes we make. We will obtain your consent to any material Privacy Policy changes if and where this is required by data protection laws applicable to us.

You can see when this Privacy Policy was last updated by checking the “EFFECTIVE DATE” displayed at the top of this Privacy Policy. The new Privacy Policy will apply to all current and past users of the website and will replace any prior notices that are inconsistent with it.

## **15. How to Contact Us**

If you require any more information or have any questions about our privacy policy, please feel free to contact us by email at [privacy@inkeep.com](mailto:privacy@inkeep.com).