Privacy Policy

Welcome, and thank you for your interest in Capcade (“Capcade”, “we,” or “us”). This Privacy Policy (‘’Policy’’) describes the types of information we gather through Capcade Services, how we use and disclose that information and the steps we take to protect it. This Policy applies to all Users of our Platform, including our website at https://www.capcade.com (the “Site”) and all related services (collectively referred to as the ‘’Capcade Services’’).

This Policy is incorporated into, and is subject to, the Capcade Terms of Service. By using Capcade Services and/or accepting the Terms of Service, you confirm that you have read and agree to this Policy.

Capitalized terms used but not defined in this Policy have the meaning given to them in the Capcade Terms of Service.

1. Definitions

AI Features

Features of the Capcade Services that use artificial intelligence, machine learning, large language models, or similar automated inference technologies to generate, summarize, classify, extract, or otherwise produce an AI Output, as further described in the Capcade AI Terms of Service.

AI Input

Any Client Data, prompt, instruction, or other information submitted to an AI Feature.

AI Output

The response, suggestion, summary, classification, or other content returned by an AI Feature.

Capcade

Capcade Inc., a corporation established under the laws of the State of Delaware (United States of America), with a registered address at 8 The Green, Ste A, Dover, DE 19901, USA, together with its wholly owned subsidiaries.

Client

An Entity or User who accepts the Capcade Terms of Service

Client Data

Files and any other digital data and information, which are subjected to the Capcade Services or otherwise inserted to the System by the Client

Personal Data

Any information relating to an identified or identifiable natural person

Public Area

The area of the Site that can be accessed both by Users and Visitors, without needing to log in

Restricted Area

The area of the Site that can be accessed only by Users, and where access requires logging in

Third-Party AI Provider

A third-party vendor that provides the underlying model or inference capability used by one or more AI Features.

User

An Entity User or Guest User

Visitor

An individual other than a User, who uses the public area, but has no access to the restricted areas of the Site

The Information We Collect

We collect various types of information from or through the Capcade Services. The legal bases for Capcade's processing of Personal Data are primarily that the processing is necessary for providing the Capcade Services in accordance with Capcade's Terms of Service and that the processing is carried out in Capcade's legitimate interests, which are further explained in Section 4 [How We Use The Information We Collect] of this Policy. We may also process data upon your consent, asking for it as appropriate.

1.1 User-provided Information

When you use the Capcade Services, as a User or as a Visitor, you may provide, and we may collect Personal Data. Examples of Personal Data include name, email address, mailing address, mobile phone number and credit card or other billing information. Personal Data also includes other information, such as geographic area or preferences, when any such information is linked to information that identifies a specific individual. You may provide us with Personal Data in various ways on the Capcade Services. For example, when you register for a Profile, use the Capcade Services, post Client Data, interact with other Users of the Capcade Services through communication or messaging capabilities, or send us customer service-related requests.

1.2 Information Collected by Clients

A Client or User may store or upload into the Capcade Services Client Data. Capcade has no direct relationship with the individuals whose Personal Data it hosts as part of Client Data. Each Client is responsible for providing notice to its customers and third persons concerning the purpose for which Client collects their Personal Data and how this Personal Data is processed in or through the Capcade Services as part of Client Data.

1.3 "Automatically Collected" Information

When a User or Visitor uses the Capcade Services, we may automatically record certain information from the User's or Visitor's device by using various types of technology, including cookies, "clear gifs" or "web beacons." This "automatically collected" information may include IP address or other device address or ID, web browser and/or device type, the web pages or sites visited just before or just after using the Capcade Services, the pages or other content the User or Visitor views or interacts with on the Capcade Services, and the dates and times of the visit, access, or use of the Capcade Services. We also may use these technologies to collect information regarding a Visitor or User's interaction with email messages, such as whether the Visitor or User opens, clicks on, or forwards a message.

1.4 Integrated Services

You may be given the option to access or register for the Capcade Services through the use of your user name and passwords for certain services provided by third parties (each, an "**Integrated Service**"), such as through the use of your Google account, or otherwise have the option to authorize an Integrated Service to provide Personal Data or other information to us. By authorizing us to connect with an Integrated Service, you authorize us to access and store your name, email

address(es), date of birth, current city, profile picture URL and other information that the Integrated Service makes available to us, and to use and disclose it in accordance with this Policy. You should check your privacy settings on each Integrated Service to understand what information that Integrated Service makes available to us and make changes as appropriate. Please review each Integrated Service's terms of use and privacy policies carefully before using their services and connecting to Capcade Services.

1.5 Information from Other Sources

We may obtain information, including Personal Data, from third parties and sources other than the Capcade Services, such as our partners, advertisers, credit rating agencies and Integrated Services. If we combine or associate information from other sources with Personal Data that we collect through the Capcade Services, we will treat the combined information as Personal Data in accordance with this Policy.

2. How We Use The Information We Collect

We use the information that we collect in a variety of ways in providing the Capcade Services and operating our business, including the following:

2.1 Operations

We use the information – other than Client Data - to operate, maintain, enhance and provide all features of the Capcade Services, to provide the services and information that you request, to respond to comments and questions and to provide support to Users of the Capcade Services. We process Client Data solely in accordance with the directions provided by the applicable Client or User.

2.2 Improvements

We use the information to understand and analyze the usage trends and preferences of our Visitors and Users, to improve the Capcade Services, and to develop new products, services, features and functionality. Should this purpose require Capcade to process Client Data, then the data will only be used in anonymized or aggregated form.

2.3 Communications

We may use a Visitor's or User's email address or other information – other than Client Data – to contact that Visitor or User (i) for administrative purposes such as customer service, to address

intellectual property infringement, right of privacy violations or defamation issues related to the Client Data or Personal Data posted on the Capcade Services or (ii) with updates on promotions and events, relating to products and services offered by us and by third parties we work with. You have the ability to opt-out of receiving any promotional communications as described below under Section 5 [Your Choices].

2.4 Cookies and Tracking Technologies

We use cookies and similar technologies like single-pixel gifs and web beacons. We use both session-based and persistent cookies. We set and access cookies on the domains operated by Capcade and its corporate affiliates (collectively, the "**Sites**"). In addition, we use third-party cookies.

Some cookies are associated with your Profile and personal information to remember that you are logged in and which workspaces you are logged into. Other cookies are not tied to your Profile but are unique and allow us to carry out analytics and customization, among other similar things. Cookies can be used to recognize you when you visit Sites or use Capcade Services, remember your preferences, and give you a personalized experience that is consistent with your settings. Cookies also make your interactions faster and more secure. To learn more about our use of cookies, please read our Cookie Policy.

2.5 Analytics

We use Google Analytics to measure and evaluate access to and traffic on the Public Area of the Site and create user navigation reports for our Site administrators. Google operates independently from us and has its own privacy policy. To learn more about Google Analytics' data privacy and security and to review their privacy policy, click here.

We also use Mixpanel to analyze product usage, understand user interactions, and improve overall user experience. Mixpanel operates independently and maintains its own privacy policy. For more information, please visit: https://mixpanel.com/legal/privacy-policy/

Datadog is a monitoring and analytics tool for information technology and DevOps teams that can be used to determine performance metrics as well as event monitoring for infrastructure and cloud services. The software can monitor services such as servers, databases and tools. For more information on Datadog's privacy policy, please visit: https://www.datadoghq.com/legal/privacy/.

We take measures to protect the technical information collected by our use of Google Analytics, Mixpanel, and Datadog. The data collected will only be used on a need-to-know basis to resolve

technical issues, administer the Site, monitor performance, and identify visitor and user preferences. Where applicable, the data is used in aggregated or non-identifiable form. We do not use any of this information to directly identify Visitors or Users.

3. To Whom We Disclose Information

Except as described in this Policy, we will not intentionally disclose the Personal Data or Client Data that we collect or store on the Capcade Services to third parties without the consent of the applicable Visitor, User or Client. We may disclose information to third parties if you consent to us doing so, as well as in the following circumstances:

3.1 Unrestricted Information

Any information that you voluntarily choose to include in a Public Area of the Capcade Services, such as a public Profile page, will be available to any Visitor or User who has access to that content.

3.2 Other Users in Your Company Profile

Certain information about your use of the Capcade Services is available to the Entity Admin of your Capcade Profile and to other Users for the purposes of providing the Capcade Services.

In addition, the Entity Admin may have access to User activity logs within the Capcade Services, including details about login activity, file access and other actions taken on the Platform.

Depending on the settings chosen by the Client, Entity Admin may have access to the content of User chats. If the Client configures such a setting, it is solely the Client's responsibility to ensure that such access is permitted under the applicable laws in the jurisdiction in which it operates. It is also the Client's sole responsibility to notify its Users that their information, including chat content and activity logs, may be accessed by Entity Admins. Capcade is not responsible for any breach of privacy or legal violations resulting from such access.

3.3 Service Providers

We work with third-party service providers as ''subprocessors'' who assist us in delivering, developing, and maintaining the Capcade Services. These subprocessors may have access to or process Personal Data or Client Data strictly as part of providing these services for us.

We limit the information provided to these service providers to the minimum necessary for them to perform their specific functions. In accordance with our Terms of Service, we ensure that all

subprocessors adhere to appropriate safeguards, including confidentiality obligations, and take appropriate technical and organizational measures to protect Personal Data or Client Data they process.

We ensure that any data transfers to affiliated entities or third-party service providers, including those located outside the European Economic Area (EEA), are subject to appropriate safeguards. These safeguards include, where applicable, the use of legally recognized mechanisms such as the EU Commission's Standard Contractual Clauses or other lawful data transfer frameworks designed to ensure an adequate level of data protection.

For a complete and up-to-date list of our subprocessors, please refer to our List of Subprocessors. You may also subscribe to receive notifications of any changes to our subprocessors, as outlined in our Terms of Service.

We will provide at least 10 business days' advance notice before engaging any new subprocessors under this general authorization. This notice will be sent to those who have subscribed to receive updates on subprocessors. Client will have the opportunity to reasonably object to changes in accordance with applicable law. If the Client does not subscribe to receive such notifications, we are not responsible for providing any additional notice about subprocessor changes through other channels.

3.4 Non-Personally Identifiable Information

We may make certain automatically collected, aggregated, or otherwise non-personally identifiable information available to third parties for various purposes, including:

(i) compliance with various reporting obligations; (ii) for business or marketing purposes; or (iii) to assist such parties in understanding our Clients', Users' and Visitors' interests, habits, and usage patterns for certain programs, content, services and/or functionality available through the Capcade Services.

3.5 Law Enforcement, Legal Process and Compliance

We may disclose Personal Data or other information if required to do so by law or in the good-faith belief that such action is necessary to comply with applicable laws, in response to a facially valid court order, judicial or other government subpoena or warrant, or to otherwise cooperate with law enforcement or other governmental agencies.

We also reserve the right to disclose Personal Data or other information that we believe, in good

faith, is appropriate or necessary to (i) take precautions against liability, (ii) protect ourselves or others from fraudulent, abusive, or unlawful uses or activity, (iii) investigate and defend ourselves against any third-party claims or allegations, (iv) protect the security or integrity of the Capcade Services and any facilities or equipment used to make the Capcade Services available, or (v) protect our property or other legal rights, enforce our contracts, or protect the rights, property, or safety of others.

3.6 Change of Ownership

Information about Users and Visitors, including Personal Data, may be disclosed and otherwise transferred to an acquirer, successor or assignee as part of any merger, acquisition, debt financing, sale of assets, or similar transaction, as well as in the event of an insolvency, bankruptcy, or receivership in which information is transferred to one or more third parties as one of our business assets and only if the recipient of the User or Visitor Data commits to a privacy policy that has terms substantially consistent with this Privacy Policy.

Client Data may be physically or electronically transferred to an acquirer, or successor or assignee as part of any merger, acquisition, debt financing, sale of assets, or similar transaction, as well as in the event of an insolvency, bankruptcy, or receivership in which information is transferred to one or more third parties as one of our business assets, for the sole purpose of continuing the operation of the Capcade Services, and only if the recipient of the Client Data commits to a privacy policy that has terms substantially consistent with this Privacy Policy.

4. AI-Enabled Features and Data Processing

Certain features of the Capcade Services use AI-enabled functionality (“AI Features”) to support and enhance service delivery. The use of AI Features is governed by the Capcade AI Terms of Service, which are incorporated into and form part of the Capcade Terms of Service.

Categories of Data Processed: When you use AI Features, the following categories of Personal Data may be processed: (i) AI Inputs, which may include Client Data containing Personal Data; (ii) AI Outputs generated in response to such inputs; and (iii) usage, metadata, including timestamps, User identifiers, and feature interaction logs.

Purpose of Processing: Personal Data processed through AI Features is used solely for the purpose of providing the AI Features as part of the Capcade Services, including generating, summarizing, classifying, extracting, and retrieving information at the User's direction. AI inputs are not used to train AI models.

Third-Party AI Providers: To deliver AI Features, Capcade transmits AI inputs to Third-Party AI Providers that operate the underlying AI models. These providers act as subprocessors on behalf of Capcade and are bound by data processing agreements that include obligations regarding data security, confidentiality, and restrictions on the use of data for model training. The current list of subprocessors, including AI providers, is maintained in the Capcade List of Subprocessors.

Data Processing Roles: When AI Features process Client Data containing Personal Data: (a) the Client is the data controller, as it determines the purpose and means of processing by choosing to use the AI Features and submitting data for processing; (b) Capcade acts as a data processor, processing data on behalf of the Client to deliver the AI Features; and (c) the Third-Party AI Provider acts as a subprocessor, processing data on behalf of Capcade for AI model execution.

Cross-Border Data Transfers: AI Inputs may be transmitted to Third-Party AI Provider infrastructure located outside the European Economic Area (EEA). All such transfers are subject to appropriate safeguards, as approved by the European Commission.

Data Retention: AI Outputs saved within the Capcade Services as part of Client Data are retained in accordance with Section 14 [Data Retention], or until earlier deletion by the Client. AI Outputs that are not stored as Client Data are retained only for as long as the AI Feature requires to operate; where this period is adjustable, Capcade will configure it on the Client's instruction. AI Inputs and AI Outputs may be retained by Capcade and/or the applicable Third-Party AI Provider for up to 30 days for abuse monitoring, safety, and service-integrity purposes, unless a longer period is required by applicable law or to investigate a suspected violation. After the applicable retention period, the data is deleted or anonymized.

Safeguards: Capcade implements technical and organizational measures to protect Personal Data processed through AI Features, including: encryption of data in transit and at rest; access controls

restricting access to AI systems, configurations, and provider consoles to authorized personnel; contractual no-training clauses with Third-Party AI Providers ensuring that AI inputs are not used to train or improve their models; logging and monitoring of AI feature usage; and periodic review of AI-related data processing activities.

Data Breach Notification: In the event of a Personal Data breach affecting Personal Data processed through AI Features, Capcade will notify the affected Client without undue delay and, where feasible, within seventy-two (72) hours of becoming aware of the breach, in accordance with applicable data protection laws.

Data Subject Rights: Data subject rights requests relating to Personal Data processed through AI Features are handled in accordance with the processes described in this Policy. Requests from data subjects should be directed to the Clients (as data controller). Where the Client requires Capcade's assistance to fulfill such requests, Capcade will provide reasonable assistance. Where fulfillment requires action by the Third-Party AI Provider, Capcade will coordinate with the provider on behalf of the Client.

Reporting Concerns: Users may report concerns or issues related to AI Featues through Capcade's existing support channels, including by contacting privacy@capcade.com.

For additional information about how Capcade uses AI, please refer to the Capcade AI Terms of Service.

5. Your Choices

5.1 Your Rights

We respect your privacy rights and provide you with reasonable access to the Personal Data that you may have provided through your use of the Capcade Services. If you wish to access or amend any other Personal Data we hold about you, or to request that we delete or transfer any information about you that we have obtained from an Integrated Service, you may contact us as set forth in Section 18 [How To Contact Us]. At your request, we will have any reference to you deleted or blocked in our database.

You may update, correct or delete your Profile information and preferences at any time by accessing

your Profile settings page on the Capcade Services. Please note that while any changes you make will be reflected in active user databases instantly or within a reasonable period of time, we may retain all information you submit for backups, archiving, prevention of fraud and abuse, analytics, satisfaction of legal obligations or where we otherwise reasonably believe that we have a legitimate reason to do so.

You may decline to share certain Personal Data with us, in which case we may not be able to provide to you some of the features and functionality of the Capcade Services.

You may request a copy of any Personal Data we have about you. You may also have the right to request that we limit our processing of such Personal Data, as well as the right to object to our processing of such Personal Data. You may also have the right to data portability.

You can withdraw any consent to processing that you have given us and prevent further processing if there is no other legitimate ground on which Capcade can process your Personal Data.

If we have received your Personal Data in reliance on the Data Privacy Framework as further described in Section 7 [Data Privacy Framework], you may also have the right to opt-out of having your Personal Data shared with third parties and to revoke your consent to our sharing your Personal Data with third parties. You may also opt-out if your Personal Data is used for any purpose that is materially different from the purpose(s) for which it was originally collected or which you originally authorized.

To exercise your rights or if you believe your right to privacy granted by applicable data protection laws has been infringed upon, please contact us at dpo@Capcade.com. You also have a right to lodge a complaint with data protection authorities.

This provision does not apply to Personal Data that is part of Client Data. In this case, the management of the Client Data is subject to the Client's own Privacy Policy and any request for access, correction or deletion should be made to the Client responsible for the uploading and storage of such data into the Capcade Services.

5.2 Navigation Information

You may also opt-out from the collection of navigation information about your visit to the Google Analytics site by using the Google Analytics Opt-out feature.

5.3 Opting-out from Commercial Communications

If you receive commercial emails from us, you may unsubscribe at any time by following the instructions contained within the email or by sending an email to the address provided in Section 18 [How To Contact Us].

Please be aware that if you opt-out of receiving commercial emails from us or otherwise modify the nature or frequency of promotional communications you receive from us, it may take up to ten (10) business days for us to process your request. Additionally, even after you opt-out from receiving commercial messages from us, you will continue to receive administrative messages from us regarding the Capcade Services.

Capcade has no direct relationship with the Client's customers or third-party whose Personal Data it may process on behalf of a Client. An individual who seeks access, or who seeks to correct, amend, delete inaccurate data or withdraw consent for further contact should direct his or her query to the Client or User they deal with directly. If the Client requests Capcade to remove the data, we will respond to its request within thirty (30) days. We will delete, amend or block access to any Personal Data that we are storing only if we receive a written request to do so from the Client who is responsible for such Personal Data unless we have a legal right to retain such Personal Data. We reserve the right to retain a copy of such data for archiving purposes or to defend our rights in litigation. Any such request regarding Client Data should be addressed as indicated in Section 18 [How To Contact Us], and include sufficient information for Capcade to identify the Client or its customer or third-party and the information to delete or amend.

6. Third-Party Services

The Capcade Services may contain features or links to websites and services provided by third parties. Any information you provide on third-party sites or services is provided directly to the operators of such services and is subject to those operators' policies, if any, governing privacy and security, even if accessed through the Capcade Services. We are not responsible for the content or privacy and security practices and policies of third-party sites or services to which links or access are provided through the Capcade Services. We encourage you to learn about third parties' privacy and security policies before providing them with information.

7. Data Privacy Framework

Capcade maintains compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Capcade has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union in reliance to the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. Capcade has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF Principles.

If there is any conflict between the terms in this Policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles shall govern. To learn more about the Data Privacy Framework program and to view our certification, please visit Data privacy framework website.

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, Capcade commits to resolve DPF Principles-related complaints about our collection and use of your personal information. EU, and UK, and Swiss individuals with inquires or complaints regarding our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.K. DPF and the Swiss-U.S. DPF should first contact Capcade at: dpo@capcade.com

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, Capcade commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner's Office (ICO) and the Gibraltar Regulatory Authority (GRA), and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard of unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF, and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF.

The U.S. Federal Trade Commission has jurisdiction over Capcade's compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF.

Under certain conditions, more fully described here, you may invoke binding arbitration when other dispute resolution procedures have been exhausted.

We may disclose your personal data without your consent to the extent necessary in connection with

legal/prospective legal proceedings, in order to establish, exercise or defend our legal rights or in response to lawful requests from public authorities including to meet national security or law enforcement requirements. Capcade discloses personal data to third parties who reasonably need to know such data as explained in Section 4 [To Whom We Disclose Information] of this Policy. In particular, Capcade remains responsible and liable under the Data Privacy Framework Principles as described in this Section if third-party agents that it engages to process personal data on its behalf do so in a manner inconsistent with the principle, unless Capcade proves that is not responsible for the event giving rise to the damage.

8. Your California Privacy Rights

View Capcade's Privacy Notice for California Residents which supplements the information contained in this Policy and applies solely to all visitors, users, and others who reside in the State of California.

9. Interest-Based Advertising

Interest-based advertising is the collection of data from different sources and across different platforms in order to predict an individual's preferences or interest and to deliver to that individual, or his/her computer, smartphone or tablet, advertising based on his/her assumed preference or interest inferred from the collection of data pertaining to that individual or others who may have a similar profile or similar interests.

We work with a variety of third parties to attempt to understand the profiles of the individuals who are most likely to be interested in the Capcade products or services so that we can send them promotional emails or serve our advertisements to them on the websites and mobile apps of other entities.

These third parties include:

(a) advertising networks, which collect information about a person's interests when that person views or interacts with one of their advertisements;

(b) attribution partners, which measure the effectiveness of certain advertisements; and

(c) business partners, which collect information when a person views or interacts with one of their advertisements.

In collaboration with these third parties, we collect information about our customers, prospects and other individuals over time and across different platforms when they use these platforms or interact with them. Individuals may submit information directly on our Sites or on platforms run by third parties, or by interacting with us, our advertisements or emails they receive from us or from third parties. We may use special tools that are commonly used for this purpose, such as cookies, beacons, pixels, tags, mobile advertising IDs, flash cookies, and similar technologies. We may have access to databases of information collected by our business partners.

The information we or a third-party collect enables us to learn what purchases the person made, what ads or content the person sees, on which ads or links the person clicks, and other actions that the person takes on our Sites, or in response to our emails, or when visiting or using third parties' platforms.

We, or the third parties with which we work, use the information collected as described above to understand the various activities and behaviors of our customers, Site visitors and others. We, or these third parties, do this for many reasons, including:

(a) to recognize new or past visitors to our Sites;

(b) to present more personalized content;

(c) to provide more useful and relevant ads - for example, if we know what ads you are shown we can try not to show you the same ones repeatedly; and

(d) to identify visitors across devices, sales channels, third-party websites and Sites, or to display or send personalized or targeted ads and other custom content that is more focused on a person's perceived interest in products or services similar to those that we offer.

Our interest-based ads may be served to you in emails or on third-party platforms. We may serve these ads about our products or services or send commercial communications directly ourselves or through these third parties.

Visitors may opt-out of receiving interest-based advertising by advertising networks that may be delivered to them on our platform and other websites by visiting the following sites:

http://www.aboutads.info/consumers; and

http://www.networkadvertising.org

These features will opt a Visitor out of many – but not all - of the interest-based advertising activities

in which we or third parties engage.

10. Do Not Track Policy

California law requires that operators of websites and online services disclose how they respond to a Do Not Track signal. Some browsers have incorporated “Do Not Track” features. Most of these features, when turned on, send a signal or preference to the website or online service that a user visits, indicating that the user does not wish to be tracked. Because there is not yet a common understanding of how to interpret Do Not Track signals, we do not currently respond to Do Not Track signals. We continue to work with the online industry to define a common understanding of how to treat Do Not Track signals.

In the meantime, you may opt-out of receiving interest-based advertising from advertising networks that may be delivered on our platform and other websites by visiting the following websites. If you want to opt-out of this online behavioral advertising, visit the following sites:

http://www.aboutads.info/consumers, and

http://www.networkadvertising.org.

This will opt you out of many – but not all - of the interest-based advertising activities in which we or third parties engage. Choices you make may be browser and device-specific. If you delete your cookies or use a different browser or a different computer or device, you may need to update your opt-out choices. Other third-party sites provide visitors with the ability to opt-out of receiving interest-based ads on their sites that you need to control through your settings on that site. For example, to opt-out of Google’s use of your online behavior for advertising purposes, visit Google’s Ad Settings page.

11. Minors And Children’s Privacy

Protecting the privacy of young children is especially important. The Capcade Services are not directed to children under the age of 18 and we do not knowingly collect Personal Data from children under the age of 18 without obtaining parental consent. If you are under 18 years of age, then please do not use or access the Capcade Services at any time or in any manner. If we learn that Personal Data has been collected on the Capcade 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 a Profile on the Capcade Services, then you may alert us at dpo@capcade.com and request that we delete that child's Personal Data from our systems.

The Capcade Services are not intended to be used by minors and are not intended to be used to post content to share publicly or with friends. To the extent that a minor has posted such content on the Capcade Services, the minor has the right to have this content deleted or removed using the deletion or removal options detailed in this Policy. If you have any questions regarding this topic, please contact us as indicated in Section 18 [How To Contact Us]. Please be aware that, although we offer this deletion capability, the removal of content may not ensure complete or comprehensive removal of that content or information.

12. Data Security

We follow generally accepted industry standards to protect the information submitted to us, both during transmission and once we receive it. We maintain appropriate administrative, technical, and physical safeguards to protect your data against accidental or unlawful destruction, accidental loss, unauthorized alteration, unauthorized disclosure or access, misuse, and any other unlawful form of processing of the data in our possession.

We employ advanced encryption techniques, such as SSL/TLS protocols, to secure data transmitted over public networks. In addition, we apply strict access controls, including firewalls, password protection, and multi-factor authentication, to ensure that only authorized personnel can access sensitive data. We also use monitoring tools to detect and prevent potential security threats.

While we strive to use the most up-to-date security practices, no method of transmission over the Internet or method of electronic storage is completely secure. We cannot ensure or warrant the security of any information you transmit to us or store on the Capcade Services and you do so at your own risk. We also cannot guarantee that such information may not be accessed, disclosed, altered or destroyed by breach of any of our physical, technical or managerial safeguards. If you believe your Personal Data or Client Data has been compromised, please contact us as set forth in Section 18 [How To Contact Us].

If we learn of a security systems breach, we will inform you and the authorities of the occurrence of the breach in accordance with applicable law.

To learn more about our security measures, please visit our Security page.

13. Data Retention

We only retain the Personal Data and Client Data collected from a User for as long as the User's Profile is active or otherwise for a limited period of time as long as we need it to fulfill the purposes for which we have initially collected it, unless otherwise required by law. Once the purpose for processing is fulfilled, or the Profile is deactivated, we will follow the data retention and deletion practices outlined below:

- Closed Profiles: The contents of closed profiles will be deleted within 6 months of the Profile's closure date. If a Client requests early deletion, we will process the request within 1 month, in accordance with the procedures outlined in our Terms of Service.
- Backup data: Backups are retained for 30 days from the date of creation.
- Billing information: Billing and financial records are retained for a period of 1 year to comply with accounting and tax regulations. During this period, the information is securely stored and accessible only to authorized personnel.
- Legal transaction information: Information related to legal transactions between the Client and Capcade, including contracts and agreements, is retained for a period of 10 years to comply with legal obligations and to protect Capcade's legal interests.

These retention periods may be extended if required by applicable law, or for legitimate business purposes, such as dispute resolution, enforcement of our agreements or legal defense. Upon the expiration of the retention period, your data will be securely deleted or anonymized in accordance with industry standards and applicable regulations.

14. Settings

Although we may allow you to adjust your privacy settings to limit access to certain Personal Data and Client Data, please be aware that no security measures are perfect or impenetrable. We are not responsible for circumvention of any privacy settings or security measures on the Capcade Services. Additionally, we cannot control the actions of other Users with whom you may choose to share your information. Further, even after information posted on the Capcade Services is removed, caching and archiving services may have saved that information and other Users or third parties may have

copied or stored the information available on the Capcade Services. We cannot and do not guarantee that information you post on or transmit to the Capcade Services will not be viewed by unauthorized persons.

15. Data Transfer

We may transfer, process and store Personal Data we collect through the Capcade Services in centralized databases and with service providers located in the U.S. The U.S. may not have the same data protection framework as the country from which you may be using the Capcade Services. When we transfer Personal Data to the U.S., we will protect it as described in this Policy.

The Capcade Services are primarily hosted in Germany. Because of the data residency feature, there are various possible places for data storage. Regardless of the database being hosted in the EU, if you choose to use the Capcade Services from the EU or other regions of the world with laws governing data collection and use that may differ from U.S. law, then please note that you may be transferring your Client Data and Personal Data outside of those regions to the United States for storage and processing by our service providers listed here. We will comply with GDPR requirements providing adequate protection for the transfer of personal information from Europe to the U.S. Also, we may transfer your data to the U.S., the EEA or other countries or regions deemed by the European Commission to provide adequate protection of personal data in connection with storage and processing of data, fulfilling your requests, and operating the Capcade Services.

16. Data Controller And Data Processor

Capcade does not own, control or direct the use of any of the Client Data stored or processed by a Client or User via the Capcade Services. Only the Client or Users are entitled to access, retrieve and direct the use of such Client Data. Capcade is largely unaware of what Client Data is actually being stored or made available by a Client or User to the Capcade Services and does not directly access such Client Data except as authorized by the Client, or as necessary to provide Capcade Services to the Client and its Users.

Because Capcade does not collect or determine the use of any Personal Data contained in the Client Data and because it does not determine the purposes for which such Personal Data is collected, the means of collecting such Personal Data, or the uses of such Personal Data, Capcade is not acting in

the capacity of data controller in terms of the European Union's General Data Protection Regulation (Regulation (EU) 2016/679, hereinafter "GDPR") and does not have the associated responsibilities under the GDPR. Capcade should be considered only as a processor on behalf of its Clients and Users as to any Client Data containing Personal Data that is subject to the requirements of the GDPR. Except as provided in this Policy, Capcade does not independently cause Client Data containing Personal Data stored in connection with the Capcade Services to be transferred or otherwise made available to third parties, except to third-party subcontractors who may process such data on behalf of Capcade in connection with Capcade's provision of Capcade Services to Clients. Such actions are performed or authorized only by the applicable Client or User.

The Client or the User is the data controller under the GDPR for any Client Data containing Personal Data, meaning that such party controls the manner such Personal Data is collected and used as well as the determination of the purposes and means of the processing of such Personal Data.

Capcade is not responsible for the content of the Personal Data contained in the Client Data or other information stored on its servers (or its subcontractors' servers) at the discretion of the Client or User, nor is Capcade responsible for the manner in which the Client or User collects, handles disclosure, distributes or otherwise processes such information.

17. Changes And Updates To This Policy

Please revisit this page periodically to stay aware of any changes to this Policy, which we may update from time to time. If we modify the Policy, we will make it available through the Site and indicate the date of the latest revision. Your continued use of the Capcade Services after the revised Policy has become effective indicates that you have read, understood and agreed to the current version of the Policy.

18. How To Contact Us

Please contact us with any questions or comments about this Policy, your Personal Data, our use and disclosure practices or your consent choices by email at dpo@capcade.com or privacy@capcade.com.

Last update: 25 May 2026