PRIVACY POLICY

Last updated and effective: September 19, 2026 (all users)
Previous version: https://legal-archive.talkpal.ai/privacy-policy/c22e9lj893qf-privacy-policy-page.pdf (September 16, 2026)

This privacy notice for TalkPal, Inc. ("**we**," "**us**," or "**our**") is designed to provide transparency and clarity about our data practices and commitments to protecting your privacy. It describes how and why we might collect, store, use, and/or share ("**process**") your information when you use our services ("**Services**"), such as when you:

- Visit our website at https://talkpal.ai, https://app.talkpal.ai, https://business.talkpal.ai or any website of ours that links to this privacy notice
- Download and use our mobile application (Talkpal), or any other application of ours that links to this privacy notice
- Engage with us in other related ways, including any sales, marketing, or events

Our goal is to ensure you fully understand the scope of how your information is handled and your rights to manage your data when engaging with us. Questions or concerns? Contact us at privacy@talkpal.ai. You may also contact our Data Protection Officer at dataprivacy@kertos.io.

Your privacy is important to us, and we are committed to addressing any concerns you may have. Reading this privacy notice will help you understand your privacy rights and choices. If you have concerns about how we process your data, please contact us at privacy@talkpal.ai. You may also exercise your rights under applicable law, as described below.

We encourage you to periodically review this notice, as it may be updated to reflect changes in our data practices or applicable laws.

TABLE OF CONTENTS

1. WHAT INFORMATION DO WE COLLECT?
2. HOW DO WE PROCESS YOUR INFORMATION?
3. WHAT LEGAL BASES DO WE RELY ON TO PROCESS YOUR INFORMATION?
4. WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?
5. WHAT IS OUR STANCE ON THIRD-PARTY WEBSITES?
6. DO WE USE COOKIES AND OTHER TRACKING TECHNOLOGIES?

7. HOW DO WE HANDLE YOUR SOCIAL LOGINS?
8. IS YOUR INFORMATION TRANSFERRED INTERNATIONALLY?
9. HOW LONG DO WE KEEP YOUR INFORMATION?
10. HOW DO WE KEEP YOUR INFORMATION SAFE?
11. DO WE COLLECT INFORMATION FROM MINORS?
12. WHAT ARE YOUR PRIVACY RIGHTS?
13. CONTROLS FOR DO-NOT-TRACK FEATURES
14. DO UNITED STATES RESIDENTS HAVE SPECIFIC PRIVACY RIGHTS?
15. DO WE MAKE UPDATES TO THIS NOTICE?
16. HOW CAN YOU CONTACT US ABOUT THIS NOTICE?
17. HOW CAN YOU REVIEW, UPDATE, OR DELETE THE DATA WE COLLECT FROM YOU?

1. WHAT INFORMATION DO WE COLLECT?

A note on terminology. In this notice, the terms “personal information” and “personal data” are used interchangeably and refer to the same categories of information about you. “Personal information” reflects the terminology used by U.S. state privacy laws (such as the CCPA/CPRA), while “personal data” reflects the terminology used by the GDPR and UK GDPR. Where this notice references our Terms and Conditions or our Data Processing Agreement, those documents use “personal data” or “Personal Data” with the same meaning.

Personal information you disclose to us

In Short: *We collect personal information that you provide to us.*

We collect personal information that you voluntarily provide to us when you register on the Services, express an interest in obtaining information about us or our products and Services, when you participate in activities on the Services, or otherwise when you contact us.

B2B Platform. The B2B platform available at https://business.talkpal.ai is used by organizational Customers (as defined in our Terms and Conditions) and their designated Administrators to manage subscriptions, invite and remove Authorized Users, view usage data for Organizational Sub-Accounts, and handle billing. Authorized Users invited through the B2B platform access the Services through the same Site (https://app.talkpal.ai) and App used by individual users; the B2B platform itself is used only by Administrators and Customer billing contacts. Personal information collected through the B2B platform may include the Administrator’s name, email address, organizational details, billing information, and aggregated or individual usage data for Authorized Users within the organizational account. This data is processed in accordance with this Privacy Policy, any applicable Order Form, and the Data Processing Agreement available at https://talkpal.ai/data-processing-agreement.

Personal Information Provided by You. The personal information that we collect depends on the context of your interactions with us and the Services, the choices you make, and the products and features you use. The personal information we collect may include the following:

- names
- phone numbers
- email addresses
- usernames
- passwords
- contact preferences
- contact or authentication data
- billing addresses
- billing information (billing name, billing country, payment method type, payment status, and transaction identifiers). Payment card details are collected directly by our payment processors and never reach Talkpal's systems.
- user application preferences
- name shown on certificates and other personal-record artifacts
- other preferences and data related to application functionality

Sensitive Information / Special Categories of Personal Data. We do not intentionally collect or process Sensitive Personal Information as defined under the CCPA/CPRA, and we do not use or disclose Sensitive Personal Information for purposes that would require providing a 'Right to Limit' under the CCPA/CPRA. The classification of certain data as "sensitive" may vary under other applicable privacy laws; where a broader definition applies, we process such data only for the purposes described in this notice and in accordance with applicable legal requirements. While we process audio of user speech for language learning and speech recognition purposes, Talkpal does not retain audio recordings of your in-app speech, and this audio is not processed to derive biometric identifiers (such as voiceprints) and is not classified as Sensitive Personal Information under the CCPA/CPRA. The text transcript produced from your speech, and the text of your written conversations with the AI tutor, are retained for no longer than thirty-six (36) months after your last activity in that conversation and are then automatically deleted, as described in Section 9. The classification of audio data may differ under other applicable laws (such as the Illinois Biometric Information Privacy Act); for details on how we handle audio data, see the "Additional information you provide" and "Note on Category E" sections of this notice.

If you are located in the EEA, UK, or Switzerland: Talkpal does not intentionally collect or seek to collect special categories of personal data within the meaning of Article 9 GDPR (for example, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used to uniquely identify a person, health data, or data concerning a person's sex life or sexual orientation). Because our Chat, Roleplay, Debate, and similar conversation modes allow free-form input, you may choose to mention such information about yourself during a conversation with the AI. Please do not share special category data about yourself or anyone else that you do not wish to disclose. If you nonetheless choose to share such information, it is processed only as an unavoidable part of generating the immediate conversational response you requested. We do not intend to process special category data and do not derive any insight, profile, or record from it. We ask you not to share it, and we apply the safeguards described in Sections 9 and 10 (limited retention, encryption, no profiling or advertising use). We do not use such information to build a profile of you beyond your stated learning preferences, and we do not use it for targeted advertising or ad-audience segmentation.

Payment Data. Payments are processed by third-party payment processors (Stripe, Apple, Google, and PayPal for legacy subscriptions). Your full card number, expiration date, security code (CVV), and bank credentials are collected and stored directly by the applicable processor through its hosted payment forms; Talkpal does not collect, process, or store this data. We receive only limited payment-related information, such as billing name, billing country, payment status, and transaction identifiers/receipts. Where you are entitled to a refund (including statutory pro-rata refunds upon termination or withdrawal), we instruct the applicable payment processor to return the amount to your original payment method, and we share the transaction identifier and refund amount with the processor for that purpose. You can find their privacy notices here: https://stripe.com/privacy, https://www.apple.com/legal/privacy/data/, https://policies.google.com/privacy, and https://www.paypal.com/us/legalhub/privacy-full.

Social Media Login Data. We may provide you with the option to register with us using your existing social media account details, like your Google, Apple, Facebook, or other social media account. If you choose to register in this way, you grant us access to basic information as defined by the platform's privacy settings and we will collect the information described in the section called "HOW DO WE HANDLE YOUR SOCIAL LOGINS?" below.

Application Data. If you use our application(s), we also may collect the following information if you choose to provide us with access or permission:

- *Mobile Device Access.* We may request access or permission to certain features from your mobile device, including your mobile device's microphone, reminders, and other features. If you wish to change our access or permissions, you may do so in your device's settings.
- *Mobile Device Data.* We automatically collect device information (such as your mobile device ID, model, and manufacturer), operating system, version information and system

configuration information, device and application identification numbers, browser type and version, hardware model Internet service provider and/or mobile carrier, and Internet Protocol (IP) address (or proxy server). If you are using our application(s), we may also collect information about the phone network associated with your mobile device, your mobile device's operating system or platform, the type of mobile device you use, your mobile device's unique device ID, and information about the features of our application(s) you accessed.

- *Push Notifications.* We may request to send you push notifications regarding your account or certain features of the application(s). If you wish to opt out from receiving these types of communications, you may turn them off in your device's settings.
- *Other application data*. We may request additional access or permissions from your mobile devices required for the full functioning of our Services.

Sub-Account Data. If you use the Services through more than one sub-account (as described in our Terms and Conditions), each sub-account maintains its own independent data, including learning progress, conversation history, lesson completion records, proficiency assessments, language selections, and usage statistics ("Sub-Account Data"). Sub-Account Data is stored and processed separately for each sub-account and is not combined across sub-accounts. Only account-level information — such as your email address, password, display name, and general account preferences — is shared across your sub-accounts. For more information about how sub-accounts work, please refer to our Terms and Conditions.

Guest Mode (iOS). The iOS version of our App offers a Guest Mode that allows limited use of the Services without creating an account. In Guest Mode, we do not collect your name or email address. We process: (i) a device-scoped identifier used to operate your Guest Mode session and enforce its limits; (ii) the device, log, usage, approximate location (IP-derived), and security/bot-protection data described in this Section 1; and (iii) your flashcard practice activity (such as the cards you view and the answers you mark). Guest Mode does not include the AI conversation features and does not capture your voice; where you play the audio of a flashcard, the card text provided by Talkpal is converted to speech by the speech-synthesis vendors described in this Section, and no data about you other than the technical data in (ii) is shared with them for that purpose. We do not use Guest Mode data to build a profile of you. Guest Mode data is deleted from our active systems within 30 days after your last Guest Mode activity on the device, or after you register an Account or delete the App, and may persist in automated backups for up to ninety (90) days before being overwritten. Guest Mode data is not transferred to any Account you later create.

This information is primarily needed to maintain the security and operation of our application(s), for troubleshooting, enhance functionality, and for our internal analytics and reporting purposes.

All personal information that you provide to us must be true, complete, and accurate, and you

must notify us of any changes to such personal information. Failure to provide accurate information may limit your access to certain features or Services.

Additional information you provide. You may interact with Artificial Intelligence ("AI") features across different modes and features across our Services, which provides you with AI-powered feedback on and analysis of your answers, or allows you to send text or audio messages to an AI in an open-ended conversational format. We use de-identified, aggregated usage data (for example, error patterns, feature usage, and lesson performance) to develop and improve our AI models, based on our legitimate interest (Art. 6(1)(f) GDPR). Identifiers are removed before any such use. You may object at any time directly in the app or your account settings or by emailing privacy@talkpal.ai; objecting will not affect your ability to use the AI features of the Services. If you object, your usage data will be excluded from AI-model development going forward; this does not affect de-identified, aggregated datasets created before your objection. This does not apply to content generated within an Organizational Sub-Account. Where your access to the Services is provided by an organization, Talkpal processes that content as a processor on the organization's documented instructions, as described in our Data Processing Agreement. When you interact with AI features, your information may be shared with AI processing vendors such as Microsoft Azure, OpenAI, Google Cloud, Google, Apple, Amazon Web Services, Anthropic, and Inworld for the purpose of generating AI-powered responses, feedback, and language assessments. These vendors process your text and audio solely on our behalf and under our instructions as data processors/service providers. Under our agreements with these vendors, they may not use your content to train their generally available AI models. Content flagged for abuse or safety review may be analyzed by a vendor solely to detect and prevent misuse. They may temporarily retain content only for abuse monitoring, security, and compliance with applicable law, and must delete it within the timeframes specified in our data processing agreements with them. Where speech recognition or text processing is performed by your device's operating system (for example, Apple's or Google's on-device or platform services), that processing is governed by the platform provider's own terms and privacy policy rather than our data processing agreements. Where a vendor is required by law to retain data for a longer period, they may do so only to the extent necessary to comply with that legal obligation. We also use the performance monitoring service Datadog, which may receive technical and diagnostic data — including metadata about your interactions (such as timestamps, error codes, and session identifiers) — for the purpose of diagnosing errors, monitoring system performance, and maintaining service reliability. Datadog does not receive the content of your conversations or audio recordings. In addition, we use self-hosted analytics, error-tracking, and data-processing tools (such as PostHog, Metabase, and Mage AI) that run entirely on our own cloud infrastructure. Data processed through these self-hosted tools remains under Talkpal's exclusive control and is not shared with, or accessible to, the providers of those tools or any other third party. These services do not receive the content of your conversations or audio recordings. We recommend that you avoid sharing highly sensitive personal information – such as financial account numbers, government identification numbers, or medical details – when using AI features, as this information may be processed by third-party AI providers.

Service providers and human review. We engage contracted individual service providers, located in Georgia, who provide customer support, content and language review, quality assurance, and operational support under our instructions and written confidentiality obligations. In performing these tasks, they may access account data (such as name, email address, and language preferences), usage and learning-progress data, support correspondence, and — where necessary to resolve a support request or perform quality assurance — the content of your conversations. These transfers are protected by the European Commission's Standard Contractual Clauses, supplemented by a transfer impact assessment.

Some activities involve you speaking into the Talkpal app. Your audio is transmitted to these third-party AI processing providers in real time to generate speech recognition and language feedback. Talkpal does not store or retain audio recordings of your speech on our systems; audio is processed transiently and is not saved by us after the response is returned. Our AI processing vendors may temporarily retain audio as described above and as governed by our data processing agreements with them. We may analyze aggregated, de-identified insights derived from use of the Services to improve our lessons and product. This analysis may include identifying patterns, enhancing lesson personalization, and generating aggregated insights to refine our offerings. If you choose to opt out of certain features, note that it may limit your access to specific functionalities designed to enhance the learning experience. You may skip speaking activities. In Photo Mode, users describe images provided by Talkpal; users do not upload photographs or images.

Information automatically collected

In Short: *Some information — such as your Internet Protocol (IP) address and/or browser and device characteristics — is collected automatically when you visit our Services.*

We automatically collect certain information when you visit, use, or navigate the Services. This information does not reveal your specific identity (like your name or contact information) but may include device and usage information, such as your IP address, browser and device characteristics, operating system, language preferences, referring URLs, device name, country, city, location, information about how and when you use our Services, and other technical information. We may also collect metadata associated with your interactions, such as timestamps and usage frequency, to monitor system performance and improve user experience. This information is primarily needed to maintain the security and operation of our Services, and for our internal analytics and reporting purposes.

Like many businesses, we also collect information through cookies and similar technologies. These technologies allow us to provide you with a seamless experience by remembering your preferences, optimizing content delivery, and personalizing your interactions with our Services. You can find out more about this in our Cookie Notice: https://talkpal.ai/cookie-policy/.

The information we collect includes:

- *Log and Usage Data.* Log and usage data is service-related, diagnostic, usage, and performance information our servers automatically collect when you access or use our Services and which we record in log files. Depending on how you interact with us, this log data may include your IP address, device information, browser type, and settings and information about your activity in the Services (such as the date/time stamps associated with your usage, pages and files viewed, searches, and other actions you take such as which features you use), device event information (such as system activity, error reports (sometimes called “crash dumps”), and hardware settings). We use this data to analyze trends, identify issues, and ensure service continuity.

- *Device Data.* We collect device data such as information about your computer, phone, tablet, or other device you use to access the Services. Depending on the device used, this device data may include information such as your IP address (or proxy server), device and application identification numbers, location, browser type, hardware model, Internet service provider and/or mobile carrier, operating system, and system configuration information. This data enables us to optimize our Services for different device types and maintain compatibility across platforms.

- *Location Data.* We collect location data such as information about your device’s approximate location, derived from your IP address. We do not use GPS or other precise geolocation technologies. This data may be used to tailor content or Services to your region, comply with localization requirements, or ensure accurate billing information. Because we derive location only from your IP address, accuracy is limited to the city or regional level.

- *Security and Bot-Protection Data.* On selected pages and actions (for example account sign-up, login, and password reset), we use Cloudflare Turnstile, a bot-protection service provided by Cloudflare, Inc., to distinguish human users from automated bots and to protect our Services against spam, abuse, and fraudulent account creation. For this purpose, Turnstile collects limited hardware and software information, such as your IP address, browser type and settings, device characteristics, and information about your interaction with the challenge widget, and transmits this data to Cloudflare to assess whether a request is likely automated. According to Cloudflare, Turnstile does not use this data for advertising, tracking, or retargeting, and does not collect persistent identifiers to track users across websites. For more information, see Section 4 below and Cloudflare’s privacy policy at https://www.cloudflare.com/privacypolicy/. We may also compare account, device, network and payment-method characteristics across accounts to identify duplicate or linked accounts and to detect abuse of free trials, referral rewards, promotion codes and refunds.

Information collected from other sources

In Short: *We may collect limited data from public databases, marketing partners, social media platforms, and other outside sources.*

In order to enhance our ability to provide relevant marketing, offers, and services to you and update our records, we may obtain information about you from other sources, such as public databases, joint marketing partners, affiliate programs, data providers, social media platforms, and from other third parties. This information includes email addresses, phone numbers, Internet Protocol (IP) addresses, social media profiles, social media URLs, and custom profiles, for purposes of targeted advertising and event promotion. If you interact with us on a social media platform using your social media account (e.g., Google, Apple, or Facebook), we receive personal information about you such as your name, email address, profile picture, and gender (where the platform provides it). This data helps us streamline account creation, improve personalized services, and enhance user engagement. Any personal information that we collect from your social media account depends on your social media account's privacy settings. We encourage you to review and adjust these settings to align with your privacy preferences.

Information we collect during sales, business, and support interactions

If you engage with us as a prospective or existing business customer — for example, by requesting a demo, attending a sales or onboarding call, or corresponding with our team — we may collect your name, email address, phone number, company name, role, and the contents of our communications. We use a customer relationship management (CRM) platform to manage these interactions and a meeting-recording and transcription tool to record, transcribe, and take notes on sales, onboarding, and business calls. Where we record a call, we inform participants at or before the start of the call and, where required by applicable law, obtain consent before recording; you may decline to be recorded. Recordings are retained only for a limited period and then deleted, while transcripts, notes, and CRM records derived from the interaction may be retained for longer in accordance with Section 9. We carry out this processing as a controller, separately from the processing of Authorized User data described in our Data Processing Agreement.

2. HOW DO WE PROCESS YOUR INFORMATION?

In Short: *We process your information to provide, improve, and administer our Services, communicate with you, for security and fraud prevention, and to comply with law. We may also process your information for other purposes with your consent.*

We process your personal information for a variety of reasons, depending on how you interact with our Services, including:

- **To facilitate account creation and authentication and otherwise manage user accounts.** We may process your information so you can create and log in to your account, as well as keep your account in working order.
- **To deliver and facilitate delivery of services to the user.** We may process your information to provide you with the requested service.
- **To respond to user inquiries/offer support to users.** We may process your information to respond to your inquiries and solve any potential issues you might have with the requested service.
- **To manage and record our business communications.** We may process your information, including by recording and transcribing sales, onboarding, or business calls, to manage our relationships with prospective and existing business customers, support and train our team, and keep accurate records of our communications.
- **To send administrative information to you.** We may process your information to send you details about our products and services, changes to our terms and policies, and other similar information.
- **To fulfill and manage your orders.** We may process your information to fulfill and manage your orders, payments, returns, and exchanges made through the Services.
- **To request feedback.** We may process your information when necessary to request feedback and to contact you about your use of our Services.
- **To send you marketing and promotional communications.** Where you have signed up for Talkpal, we may email you about Talkpal's own similar products and services, new features, and learning tips, based on the customer-relationship exemption under applicable electronic-communications laws, or based on your consent where required by law or where we have obtained it. We inform you of this at sign-up, and you can object or unsubscribe at any time, free of charge, via the unsubscribe link in every email or in your account settings. For more information, see "WHAT ARE YOUR PRIVACY RIGHTS?" below.
- **To deliver targeted advertising to you.** We may process your information to develop and display personalized content and advertising tailored to your interests, location, and more. For more information see our Cookie Notice: https://talkpal.ai/cookie-policy/.
- **To protect our Services.** We may process your information as part of our efforts to keep our Services safe and secure, including fraud monitoring and prevention and distinguishing human users from automated bots (for example, through Cloudflare Turnstile on selected pages and actions).
- **To identify usage trends.** We may process information about how you use our Services to better understand how they are being used so we can improve them.

- **To determine the effectiveness of our marketing and promotional campaigns.** We may process your information to better understand how to provide marketing and promotional campaigns that are most relevant to you.
- **To estimate the expected value of a subscription for advertising measurement.** We use an automated model to estimate, from account and usage data (not conversation content), how likely a new subscription is to convert to a paid plan, and we send that estimated value together with the conversion event to our advertising partners so we can measure and bid on our campaigns more accurately. This does not affect your price, features, or access. This is a form of profiling for marketing purposes, based on our legitimate interests; you can object at any time in your account settings, after which we send conversion events without a modeled value.
- **To save or protect an individual's vital interest.** We may process your information when necessary to save or protect an individual's vital interest, such as to prevent harm.
- **To provide personalized feedback for the functioning of our app.** We may process, analyze and use any additional information you provide to us while using our Services or communicating with Artificial Intelligence ("AI").
- **To Improve User Experience.** We may process your information to personalize and optimize your experience on our Services, such as by tailoring content recommendations, user interfaces, and app functionality to your preferences.
- **To Conduct Research and Development.** We may process your information to perform data analysis, testing, and research that help us develop and improve new products, features, and services.
- **To Comply with Legal Obligations.** We may process your information to comply with applicable legal requirements, such as responding to court orders, subpoenas, or regulatory inquiries.
- **To Monitor and Enforce Our Terms and Policies.** We may process your information to detect and prevent violations of our terms and conditions, ensure compliance with our policies, and protect the integrity of our platform.
- **To Provide Service Notifications and Alerts.** We may process your information to send you notifications about important service updates, such as security alerts, downtime notifications, or significant changes to your account, as well as billing and subscription communications — including subscription renewal reminders, trial-expiry notices, price-change notices, payment-failure notices, invoices and receipts, and confirmations of cancellation, termination, or withdrawal. These are service communications necessary for the administration of your subscription, not marketing.

- **To respond to safety risks.** Our AI features are instructed to recognise mentions of suicide or self-harm and direct you to crisis resources. We do not scan, score or profile you, and build no mental-health profile.

- **To determine and honor statutory consumer rights that depend on your country of residence** (for example cancellation, termination, withdrawal, and refund rights), we process your billing country and related account and transaction details. Where you exercise such a right — by email to support@talkpal.ai, through your account settings, or through any online cancellation function we make available — we additionally process the information you provide for that purpose: your name, the email address associated with your account, the designation of your subscription, the type of and (where you provide one) the reason for your termination, your requested effective date, and the date and time we received your declaration, together with our confirmations to you.

Profiling and automated decision-making. We do not make decisions based solely on automated processing, including profiling, that produce legal effects concerning you or similarly significantly affect you. Where we process your information on the basis of our legitimate interests, you may object to such processing, including any profiling based on it, at any time by contacting us at privacy@talkpal.ai or, where available, in your account settings. Objecting does not affect your ability to use the Services.
Objecting does not switch off the learning feedback that is part of the Services themselves. Our AI necessarily analyzes what you write and say in order to give you language-learning feedback, such as corrections of grammar, vocabulary and pronunciation, and to adapt exercises to your level. This processing is necessary to provide the Services you have requested (Art. 6(1)(b) GDPR) and is not used to make decisions with legal or similarly significant effects. If you disagree with a specific piece of feedback or an assessment of your level, you may contact us at support@talkpal.ai and a member of our team will review it and respond; we do not otherwise review your conversations in real time.

3. WHAT LEGAL BASES DO WE RELY ON TO PROCESS YOUR INFORMATION?

In Short: *We only process your personal information when we believe it is necessary and we have a valid legal reason (i.e., legal basis) to do so under applicable law, like with your consent, to comply with laws, to provide you with services to enter into or fulfill our contractual obligations, to protect your rights, or to fulfill our legitimate business interests. We ensure that these legal bases are applied consistently, transparently, and in a manner that respects your privacy.*

If you are located in the EU or UK, this section applies to you.

The General Data Protection Regulation (GDPR) and UK GDPR require us to explain the valid

legal bases we rely on in order to process your personal information. As such, we may rely on the following legal bases to process your personal information:

- **Consent.** We may process your information if you have given us permission (i.e., consent) to use your personal information for a specific purpose. This consent will always be informed, freely given, and explicit where required by law. This includes consent for non-essential cookies, SDKs, and device identifiers (see Section 6) and for audience matching with advertising partners (see Section 4). You can withdraw your consent at any time as described in Section 12.
- **Performance of a Contract.** We may process your personal information when we believe it is necessary to fulfill our contractual obligations to you, including providing our Services or at your request prior to entering into a contract with you. This includes enabling core functionalities of our Services or delivering personalized features based on your usage.
- **Legitimate Interests.** We may process your information when we believe it is reasonably necessary to achieve our legitimate business interests and those interests do not outweigh your interests and fundamental rights and freedoms. For example, we may process your personal information for some of the purposes described in order to:
  - Email users about Talkpal's own similar products and services, new features, special offers, and learning tips, as disclosed at sign-up and subject to your right to object at any time, free of charge
  - Develop and display personalized and relevant advertising content for our users
  - Analyze how our Services are used so we can improve them to engage and retain users
  - Support our marketing activities
  - Estimate the expected value of a subscription for advertising measurement, subject to your right to object at any time
  - Diagnose problems and/or prevent fraudulent activities
  - To ensure network and information security, including preventing unauthorized access to our systems
  - Understand how our users use our products and services so we can improve user experience
  - Develop and improve our AI models using de-identified, aggregated usage data
- **Legal Obligations.** We may process your information where we believe it is necessary for compliance with our legal obligations, such as to cooperate with a law enforcement body or regulatory agency, exercise or defend our legal rights, or disclose your information as evidence in litigation in which we are involved. This also includes compliance with statutory

consumer-protection obligations — for example, receiving, processing, confirming, and keeping records of subscription cancellation, termination, and withdrawal requests and the related refunds, including under § 312k of the German Civil Code (BGB) and equivalent laws of your country of residence.

- **Vital Interests.** We may process your information where we believe it is necessary to protect your vital interests or the vital interests of a third party, such as responding to emergencies, or addressing situations involving immediate threats to life or safety.

- **Organizational Accounts and Data Controller Roles.** Where a Customer subscribes to the Services on behalf of its Authorized Users under Section 1A of our Legal Terms, the Customer acts as the data controller and Talkpal acts as the data processor with respect to the personal data of its Authorized Users that is processed within the Organizational Sub-Account. In such cases, Talkpal processes personal data on behalf of the Customer in accordance with these Legal Terms, any applicable Order Form, and the Data Processing Agreement available at https://talkpal.ai/data-processing-agreement. If you are an Authorized User and have questions about how your organization handles your data, we recommend contacting your organization's Administrator directly. Talkpal will support your organization in responding to such requests in accordance with the Data Processing Agreement. For your Personal Sub-Account, Talkpal is the data controller. Talkpal also acts as an independent data controller for: (i) your Account-Level Information — your email address, password, display name, and general account preferences — including where your Account was created by accepting an organization's invitation; and (ii) billing and payment data connected with an organization's subscription, which Talkpal processes for invoicing, payment collection, fraud prevention, and compliance with its own legal obligations under tax, accounting, and financial regulations. Where an organization invites you to join its account, Talkpal processes the contact details the organization provides (such as your name and email address) on the organization's behalf, solely to deliver and administer the invitation; once you accept the invitation and create or link your Account, Talkpal processes your Account-Level Information as an independent controller.

If you are located in Canada, this section applies to you.

We may process your information if you have given us specific permission (i.e., express consent) to use your personal information for a specific purpose, or in situations where your permission can be inferred (i.e., implied consent). In either case, we ensure that the consent is consistent with Canadian privacy laws and principles. You can withdraw your consent at any time.

In some exceptional cases, we may be legally permitted under applicable law to process your information without your consent, including, for example:

- If collection is clearly in the interests of an individual and consent cannot be obtained in a timely way

- For investigations and fraud detection and prevention
- For business transactions provided certain conditions are met, such as due diligence processes during mergers or acquisitions
- If it is contained in a witness statement and the collection is necessary to assess, process, or settle an insurance claim
- For identifying injured, ill, or deceased persons and communicating with next of kin
- If we have reasonable grounds to believe an individual has been, is, or may be victim of financial abuse
- If it is reasonable to expect collection and use with consent would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province
- If disclosure is required to comply with a subpoena, warrant, court order, or rules of the court relating to the production of records
- If it was produced by an individual in the course of their employment, business, or profession and the collection is consistent with the purposes for which the information was produced
- If the collection is solely for journalistic, artistic, or literary purposes
- If the information is publicly available and is specified by the regulations

4. WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?

In Short: *We may share information in specific situations described in this section and/or with the following categories of third parties.*

Vendors, Consultants, and Other Third-Party Service Providers. We may share your data with third-party vendors, service providers, contractors, or agents ("**third parties**") who perform services for us or on our behalf and require access to such information to do that work. Each third party is subject to strict contractual obligations that mandate the safeguarding, confidentiality, and proper use of your personal data. We have contracts in place with our third parties, which are designed to help safeguard your personal information. These agreements explicitly prohibit the unauthorized use, sharing, or retention of your personal data and require third parties to implement robust security measures aligned with industry standards. This means that they cannot do anything with your personal information unless we have instructed them to do it. They will also not share your personal information with any organization apart from us. They also commit to protect the data they hold on our behalf and to retain it for the

period we instruct. The categories of third parties we may share personal information with are as follows:

- Ad Networks
- Affiliate Marketing Programs
- Cloud Computing Services
- Communication & Collaboration Tools
- Customer Support & Ticketing Tools
- Data Analytics Services
- Data Storage Service Providers
- Finance & Accounting Tools
- Payment Processors
- Performance Monitoring Tools
- Product Engineering & Design Tools
- Retargeting Platforms
- Sales & Marketing Tools
- Social Networks
- A/B Testing Tools
- Testing Tools
- User Account Registration & Authentication Services
- Website Hosting Service Providers
- Cookie Management Tools
- Customer Relationship Management (CRM) Tools
- Meeting Recording and Transcription Tools
- Content Delivery Networks (CDN)
- Security & Fraud Detection Services
- Educational Technology Platforms

- Business Intelligence Tools
- Ad Fraud Detection Services
- Personalization Engines

Audience Matching for Advertising (Lookalike and Custom Audiences). With your consent, we may share a limited set of identifiers derived from your account data (for example, a cryptographically hashed version of your email address) with our advertising partners (including Meta, Google, OpenAI Ads, Taboola, and TikTok) so that they can (i) recognize you as an existing Talkpal user for measurement purposes, and (ii) build "lookalike" or "custom" audiences of other users who share similar characteristics, for the purpose of showing Talkpal advertising to prospective users. This processing is separate from, and in addition to, our use of cookies and advertising SDKs described in Section 6 and our Cookie Notice. For users in the EEA, UK, and Switzerland, this takes place only where you have given consent under Art. 6(1)(a) GDPR (in conjunction with § 25(1) TDDDG or the equivalent provision under applicable national law). You can withdraw your consent at any time via our cookie banner (consent preference settings) or by contacting us at privacy@talkpal.ai, and you can separately object to this processing at any time free of charge (see "WHAT ARE YOUR PRIVACY RIGHTS?" in Section 12).

Attribution and campaign measurement (AppsFlyer). We use AppsFlyer Inc. (100 1st Street, 25th Floor, San Francisco, CA 94105, USA) as our mobile measurement partner to measure app installs and in-app events and to attribute them to our advertising campaigns. For this purpose, AppsFlyer processes device identifiers (such as the IDFA or GAID, where permitted), IP address, and technical and usage/event data. AppsFlyer does not receive the content of your conversations. Where AppsFlyer measures in-app usage on our behalf, it acts as our data processor; where we use AppsFlyer data for our own advertising attribution and campaign measurement, we act as an independent controller. For users in the EEA, UK, and Switzerland, attribution using device identifiers takes place only where you have given consent (Art. 6(1)(a) GDPR in conjunction with § 25(1) TDDDG or the equivalent national provision), which you can withdraw at any time via our consent preference settings, your device settings, or by contacting privacy@talkpal.ai. AppsFlyer processes data in the United States; these transfers are safeguarded as described in Section 8 ("IS YOUR INFORMATION TRANSFERRED INTERNATIONALLY?") of this policy.

Website analytics, advertising measurement and affiliate tracking. On our marketing website (talkpal.ai and its subdomains) we use, subject to your consent under our cookie banner, third-party services for web analytics and session analytics, advertising conversion measurement and remarketing (including pixels and tags of advertising and social-media platforms), and affiliate-partner conversion tracking used to calculate partner commissions. Some of these events are relayed through a first-party server-side tagging endpoint operated by us before being forwarded to the respective provider; this does not change the recipient or the legal basis. Embedded third-party content (for example, scheduling widgets) loads only after you

consent to the corresponding cookie category. The current list of providers, cookies, purposes and storage durations is maintained in our Cookie Notice at https://talkpal.ai/cookie-policy/ and can be reviewed and changed at any time via “Cookie Preferences” in the footer.

Bot and abuse protection (Cloudflare Turnstile). We use bot-protection and fraud-detection services, including Turnstile, a service provided by Cloudflare, Inc., 101 Townsend St, San Francisco, CA 94104, USA (“Cloudflare”), and comparable services from other providers listed in our Cookie Notice, on selected pages and actions of our Services (such as account sign-up, login, and password reset) to protect against bots, spam, and abusive or fraudulent requests. For this purpose, Turnstile processes your IP address, browser and device information, and information about your interaction with the challenge widget, and transmits this data to Cloudflare for risk analysis. Turnstile issues a token indicating whether a request likely originates from a human; we use this result solely to decide whether to allow, challenge, or block the request. According to Cloudflare, Turnstile data is not used for advertising, tracking, or retargeting, and Turnstile does not collect persistent identifiers to track users across websites. The legal basis for this processing is our legitimate interest in ensuring the security and integrity of our Services and preventing fraud and abuse (Art. 6(1)(f) GDPR). Cloudflare may process this data on servers in the United States; these transfers are safeguarded as described in Section 8 (“IS YOUR INFORMATION TRANSFERRED INTERNATIONALLY?”), including Cloudflare’s certification under the EU-U.S. Data Privacy Framework. Further information: https://www.cloudflare.com/privacypolicy/.

Social Media Online Presences

Purpose: Communication with prospective and existing users, provision of information about our products and services, and analysis of the use of our online presences.

Recipients:

- Meta Platforms Ireland Ltd., Merrion Road, Dublin 4, D04 X2K5, Ireland (“Facebook,” “Instagram,” and “Threads”)
- LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland (“LinkedIn”)
- Google Ireland Limited, Gordon House, 4 Barrow St, Dublin, D04 E5W5, Ireland (“YouTube”)
- TikTok Technology Limited, 10 Earlsfort Terrace, Dublin 2, D02 T380, Ireland (“TikTok”)
- X Internet Unlimited Company, One Cumberland Place, Fenian Street, Dublin 2, D02 AX07, Ireland (“X”)
- Reddit, Inc., 548 Market Street, PMB 16093, San Francisco, CA 94104, United States (“Reddit”)

- Spotify AB, Regeringsgatan 19, 111 53 Stockholm, Sweden (“Spotify” – advertising pixel)

Data Processed:

- Demographic information (e.g., age, gender)
- Professional information where applicable (e.g., industry, professional experience)
- Interaction data (e.g., likes, shares, comments, follows, reposts)
- Usage statistics (e.g., page views, video views, reach, impressions)
- Content preferences (e.g., popular topics, interests)

Joint Controllership with LinkedIn and Meta: With regard to the processing of statistical usage data relating to our presences on LinkedIn, Facebook, and Instagram (so-called “Page Insights”), we and LinkedIn Ireland Unlimited Company and Meta Platforms Ireland Limited respectively act as joint controllers within the meaning of Art. 26 GDPR. The joint controllership relates in particular to the collection and evaluation of usage data for the purpose of generating page statistics, while LinkedIn and Meta assume primary responsibility for facilitating the exercise of data subject rights and fulfilling information obligations. The key elements of the respective joint controllership arrangements (in particular regarding the allocation of responsibilities and the handling of data subject rights) can be found in LinkedIn’s Joint Controller Addendum and Meta’s Page Controller Addendum (see the privacy notices of the respective platforms). For our presences on YouTube, TikTok, **and X**, the respective platform operators act as independent controllers for the data they collect and process in connection with our presence.

Legal Basis:

- Art. 6(1)(b) GDPR (performance of a contract and pre-contractual measures)
- Art. 6(1)(f) GDPR (legitimate interest in effective information and communication)

Retention Period: In accordance with the privacy policies of the respective platforms.

Further Information:

Meta (Facebook, Instagram, Threads):

- https://www.facebook.com/legal/terms/information_about_page_insights_data
- https://www.facebook.com/legal/terms/page_controller_addendum
- https://www.facebook.com/privacy/policy/

- https://privacycenter.instagram.com/policy/

LinkedIn:

- https://legal.linkedin.com/pages-joint-controller-addendum
- https://www.linkedin.com/legal/privacy-policy

YouTube:

- https://policies.google.com/privacy

TikTok:

- https://www.tiktok.com/legal/page/eea/privacy-policy/en

X:

- https://x.com/en/privacy

Reddit:

- https://www.reddit.com/policies/privacy-policy

Note: We have no influence over the independent data processing carried out by the platform operators. When you visit our online presences, usage data may be transmitted to the operators, who may use it for their own purposes. Data subject rights may be exercised directly against the platform operators.

We also may need to share your personal information in the following situations:

- **Business Transfers.** We may share or transfer your information in connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of our business to another company. In such instances, we will make reasonable efforts to ensure that the recipient of your personal data is bound by privacy obligations consistent with this notice.
- **Affiliates.** We may share your information with our affiliates, in which case we will require those affiliates to honor this privacy notice. Affiliates include our parent company and any subsidiaries, joint venture partners, or other companies that we control or that are under common control with us.
- **Business Partners.** We may share your information with our business partners to offer you certain products, services, or promotions. These partnerships are subject to confidentiality

agreements, and we ensure that your information is shared solely for the intended purposes outlined in our agreements.

- **Referral Program.** Where you participate in our referral program, limited information about your referrals (such as a referred sign-up status, or reward redemption status) may be shown to the referring user. We do not share contact details such as email addresses or phone numbers between referrer and referee unless the user voluntarily provides them.
- **Organizational Administrators.** If you access the Services through an Organizational Sub-Account (as described in our Terms and Conditions), your Sub-Account Data generated within that Organizational Sub-Account – including but not limited to lesson completion, time spent, language proficiency progress, and activity logs – may be visible to the Customer's designated Administrator(s). This visibility is limited to data generated within the applicable Organizational Sub-Account. Your Personal Sub-Account Data and any Sub-Account Data associated with a different Customer's Organizational Sub-Account are not accessible to any Administrator. The Customer is responsible for its own use of this data in compliance with applicable law.

5. WHAT IS OUR STANCE ON THIRD-PARTY WEBSITES?

In Short: *We are not responsible for the safety of any information that you share with third parties that we may link to or who advertise on our Services, but are not affiliated with, our Services.*

The Services may link to third-party websites, online services, or mobile applications and/or contain advertisements from third parties that are not affiliated with us and which may link to other websites, services, or applications. While we strive to link only to reputable third parties, we cannot monitor or control their actions, content, or data practices. Accordingly, we do not make any guarantee regarding any such third parties, and we will not be liable for any loss or damage caused by the use of such third-party websites, services, or applications. We encourage you to approach interactions with third-party websites or applications cautiously, especially if providing personal or sensitive data. The inclusion of a link towards a third-party website, service, or application does not imply an endorsement by us. We cannot guarantee the safety and privacy of data you provide to any third parties. Before sharing your personal information, you should investigate how those third parties will handle your data, including reviewing their privacy policies and security measures. Any data collected by third parties is not covered by this privacy notice. We are not responsible for the content or privacy and security practices and policies of any third parties, including other websites, services, or applications that may be linked to or from the Services. You should review the policies of such third parties and contact them directly to respond to your questions. If you suspect misuse or improper handling of your data by a third party linked to our Services, we recommend notifying the third party directly and reporting any concerns to us at privacy@talkpal.ai for review.

6. DO WE USE COOKIES AND OTHER TRACKING TECHNOLOGIES?

In Short: *We may use cookies and other tracking technologies to collect and store your information.*

We may use cookies and similar tracking technologies (like web beacons and pixels) to access or store information across our websites, including https://talkpal.ai, https://app.talkpal.ai, and https://business.talkpal.ai. The types of cookies used may vary by domain — for example, our marketing website may use advertising and analytics cookies, while our application and B2B platform primarily use functional and session cookies necessary for the operation of the Services. Specific information about how we use such technologies and how you can refuse certain cookies is set out in our Cookie Notice: https://talkpal.ai/cookie-policy/. You can manage or disable cookies through your browser settings; however, please note that certain features of our Services may become limited or unavailable if cookies are blocked.

Legal basis for cookies, SDKs, and similar technologies. Where the storage of, or access to, information on your device (for example via cookies, advertising identifiers such as IDFA/GAID, SDKs, or similar technologies) is not strictly necessary to provide the service you requested, we rely on your consent under Art. 6(1)(a) GDPR, given in accordance with applicable national implementing legislation of the ePrivacy Directive (including § 25 TDDDG in Germany). You can give or withdraw this consent at any time through our cookie preference settings.

We are committed to transparency regarding our use of tracking technologies and encourage you to familiarize yourself with our Cookie Notice for detailed guidance.

7. HOW DO WE HANDLE YOUR SOCIAL LOGINS?

In Short: *If you choose to register or log in to our Services using a social media account, we may have access to certain information about you.*

Our Services offer you the ability to register and log in using your third-party social media account details (like your Google, Apple, or Facebook logins). Where you choose to do this, we will receive certain profile information about you from your social media provider. The extent of information shared with us depends on your social media platform's privacy settings and permissions you grant. The profile information we receive may vary depending on the social media provider concerned, but will often include your name, email address, profile picture, and (where provided) gender, as well as other information you choose to make public on such a social media platform. We may also collect any other data explicitly shared during the login process, such as preferences or interactions tied to your social media account.

We will use the information we receive only for the purposes that are described in this privacy notice or that are otherwise made clear to you on the relevant Services. To ensure transparency, we will never post on your behalf or share your activities without your explicit

consent. Please note that we do not control, and are not responsible for, other uses of your personal information by your third-party social media provider. We strongly encourage you to regularly review and adjust your social media privacy settings to align with your preferences. We recommend that you review their privacy notice to understand how they collect, use, and share your personal information, and how you can set your privacy preferences on their sites and apps.

8. IS YOUR INFORMATION TRANSFERRED INTERNATIONALLY?

In Short: *We may transfer, store, and process your information in countries other than your own.*

Our servers are located in the European Union (including Germany, Sweden, and Ireland) and the United States. Certain service providers may access personal data from additional locations (including Australia and Georgia), as described in this policy and in our Data Processing Agreement. If you are accessing our Services from a country other than those listed above, please be aware that your information may be transferred to, stored, and processed by us and by the third parties with whom we may share your personal information (see "WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?" above) in the locations identified above and in Schedule 3 of our Data Processing Agreement. We take steps to ensure that your information is handled securely and in accordance with this privacy notice, regardless of where it is processed. This includes leveraging industry-standard encryption protocols, secure server configurations, and stringent access controls.

Where we transfer personal data outside the EEA, the UK, or Switzerland to countries that do not benefit from an adequacy decision, we rely on the European Commission's Standard Contractual Clauses (Art. 46(2)(c) GDPR) as the primary transfer mechanism. This includes transfers to our contracted service providers located in Georgia. For transfers to recipients certified under the EU-U.S. Data Privacy Framework, we rely on the adequacy decision of the European Commission (Art. 45 GDPR). For transfers subject to UK GDPR, we use the UK International Data Transfer Agreement (IDTA) or the UK Addendum to the EU SCCs, as applicable. For transfers originating in Switzerland, we rely on the EU Standard Contractual Clauses as adapted for Switzerland and recognized by the Swiss Federal Data Protection and Information Commissioner, or, for recipients certified under the Swiss-U.S. Data Privacy Framework, on the Swiss Federal Council's adequacy recognition of that framework.

If you are a resident in the European Economic Area (EEA), United Kingdom (UK), or Switzerland, then these countries may not necessarily have data protection laws or other similar laws as comprehensive as those in your country. However, we will take all necessary measures to protect your personal information in accordance with this privacy notice and applicable law.

9. HOW LONG DO WE KEEP YOUR INFORMATION?

In Short: *We keep your information for as long as necessary to fulfill the purposes outlined in this privacy notice unless otherwise required by law.*

We will only keep your personal information for as long as it is necessary for the purposes set out in this privacy notice, unless a longer retention period is required or permitted by law (such as tax, accounting, or other legal requirements). We periodically review our data retention policies to ensure compliance with changing laws and evolving best practices, minimizing unnecessary data storage. No purpose in this notice will require us keeping your personal information for longer than the period of time in which users have an account with us, plus the post-deletion retention periods described in Section 12 below. Some categories of information are kept for shorter, category-specific periods, which are set out below and take precedence over the general period stated in this paragraph. Following account deletion, personal data is purged from our active systems within thirty (30) days. Data contained in automated backups may persist for up to ninety (90) days before being overwritten in the normal course of our backup rotation.

Conversation transcripts. Text transcripts of your conversations with the AI tutor across all conversation modes — including text produced from your speech by speech recognition — are retained for no longer than thirty-six (36) months after your last activity in that conversation. At the end of that period they are automatically deleted on a rolling basis, whether or not your account is still active; we retain only aggregated statistics that cannot identify you. You can also delete all of your conversations at any time before that period ends by deleting your account or by contacting us at privacy@talkpal.ai. Audio of your speech is not stored at any point (see Section 1). For conversations within an Organizational Sub-Account, the same thirty-six (36) month deletion applies as a documented instruction under our Data Processing Agreement (Section 9.5).

Derived learning data. Data derived from your use of the Services that does not contain conversation content — for example your proficiency level, assessment results, feedback and scores, lesson-completion records, progress data and certificates issued — is retained for as long as your account is active, so that the continuity of your learning record is preserved for the duration of your learning journey, and is then deleted in accordance with the post-deletion periods described above and in Section 12.

Recordings of sales, onboarding, or business calls are retained only for a limited period and then deleted, although transcripts, notes, or CRM entries derived from those calls may be retained for longer as described in this notice. For complete details on post-deletion retention, see Section 12. Organizational Sub-Account Data. When an Organizational Sub-Account is deactivated — whether due to the Customer's subscription expiring, the Administrator removing the user, or the user voluntarily leaving the organizational account — we will delete the Sub-Account Data associated with that Organizational Sub-Account within thirty (30) days, unless: (a) retention for a longer period is required by applicable law; or (b) the data is subject to an

ongoing legal hold, investigation, or dispute. The user's Account, account-level information, and data associated with other sub-accounts (including the Personal Sub-Account) are not affected by this deletion. However, certain data, such as payment records or transaction details, may be retained for longer durations to comply with legal or regulatory requirements. Where you act on behalf of a business customer (for example as an Administrator or billing contact), we retain the organizational account record — your business contact details, the order form, invoices, and our records of contract acceptance — for as long as needed to resolve any matters arising from the contract and thereafter only to the extent required by applicable tax, accounting, and commercial record-keeping laws, after which it is deleted or anonymized. Records of subscription cancellation, termination, withdrawal, and refund requests, together with our confirmations, are retained for as long as necessary to demonstrate compliance with applicable consumer protection and commercial record-keeping laws.

Guest Mode data. Data associated with iOS Guest Mode is deleted from our active systems within 30 days after your last Guest Mode activity on the device, or after you register an Account or delete the App (up to 90 days in automated backups), as described in Section 1.

When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymize such information, or, if this is not possible (for example, because your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible. We also ensure that any archived information is securely encrypted and inaccessible to unauthorized parties. If you have questions about specific retention periods for your personal information, or if you wish to request deletion, you may contact us at privacy@talkpal.ai.

10. HOW DO WE KEEP YOUR INFORMATION SAFE?

In Short: *We aim to protect your personal information through a system of organizational and technical security measures.*

We have implemented appropriate and reasonable technical and organizational security measures designed to protect the security of any personal information we process. These measures include, but are not limited to, encryption protocols, secure socket layer (SSL) technology, regular security audits, multi-factor authentication, and strict access controls for sensitive data. However, despite our safeguards and efforts to secure your information, no electronic transmission over the Internet or information storage technology can be guaranteed to be 100% secure, so we cannot promise or guarantee that hackers, cybercriminals, or other unauthorized third parties will not be able to defeat our security and improperly collect, access, steal, or modify your information. Although we will do our best to protect your personal information, transmission of personal information to and from our Services is at your own risk. We strongly recommend that you use strong, unique passwords for your accounts and take

additional precautions such as enabling multi-factor authentication when available. You should only access the Services within a secure environment. Avoid using public or unsecured Wi-Fi networks when accessing our Services to minimize potential risks.

Notifying you of a data breach. If a personal data breach occurs that is likely to result in a risk to your rights and freedoms, we will notify the competent supervisory authority without undue delay and, where feasible, within 72 hours of becoming aware of it, as required by Art. 33 GDPR. Where the breach is likely to result in a high risk to your rights and freedoms, we will notify you directly without undue delay, in accordance with Art. 34 GDPR and any applicable state or national breach-notification law. Notifications will describe the nature of the breach, the likely consequences, the measures we have taken, and a point of contact for further information.

11. DO WE COLLECT INFORMATION FROM MINORS?

In Short: *We do not knowingly collect data from or market to anyone under 18 years of age. If we discover that a minor's data has been collected, we will delete it and deactivate their account. By using the Services, you confirm that all information provided is accurate and truthful, including representations regarding your age.*

We do not knowingly collect personal data from, solicit data from, or market to anyone under 18 years of age. The Services are not intended for, and may not be used by, anyone under 18. We do not offer a parental consent mechanism for minors to use the Services. If we become aware that we have collected personal information from a user under the age of 18, we will promptly deactivate the account and delete the associated personal data from our records within thirty (30) days. We may implement age verification measures as required by applicable law. If you become aware that a minor under 18 has registered for or is using the Services, please contact us immediately at privacy@talkpal.ai.

This age requirement applies equally to Guest Mode on the iOS App: Guest Mode is available only to users aged 18 or over, users represent that they meet this requirement by using Guest Mode after the disclaimer displayed on entry, and we may terminate Guest Mode access and delete associated data where we reasonably believe a user is under 18.

Additional information for users in the EEA, UK, and Switzerland: We recognize that self-declared age is not, by itself, a guaranteed age-verification method. In addition to the 18+ requirement, we rely on the representation each user makes, by accepting our Terms and Conditions at registration, that they are at least 18, and may take further age-assurance steps where required by applicable law. If we become aware that we have collected personal data from any user under 18 — including a child below the relevant age of digital consent in their country of residence, which ranges from 13 to 16 years under Art. 8 GDPR — we will delete that data and deactivate the associated account without undue delay, and in any event within thirty (30) days, consistent with the practice described in this Section 11. Organizational accounts. Where

access to the Services is provided by an organization (as described in Section 1A of our Terms and Conditions), that organization is responsible, as controller, for verifying that every individual it invites is at least 18 years old, and warrants to us that it has done so. We rely on that warranty, in addition to the age confirmation each user gives when accepting our Terms. If you believe an organization has granted access to a person under 18, contact us at privacy@talkpal.ai; we will deactivate the affected sub-account and delete the associated personal data as described above, and we will notify the organization's Administrator.

12. WHAT ARE YOUR PRIVACY RIGHTS?

In Short: *In some regions, such as the European Economic Area (EEA), United Kingdom (UK), Switzerland, and Canada, you have rights that allow you greater access to and control over your personal information. You may review, change, or terminate your account at any time.*

In some regions (like the EEA, UK, Switzerland, and Canada), you have certain rights under applicable data protection laws. These may include the right (i) to request access and obtain a copy of your personal information, (ii) to request rectification or erasure; (iii) to restrict the processing of your personal information; (iv) if applicable, to data portability; and (v) not to be subject to automated decision-making. In certain circumstances, you may also have the right to object to the processing of your personal information, including profiling. You can make such a request by contacting us by using the contact details provided in the section "HOW CAN YOU CONTACT US ABOUT THIS NOTICE?" below. You can also exercise your right to object to AI-model improvement directly in the app or your account settings, without contacting us.

We will consider and act upon any request in accordance with applicable data protection laws. We strive to respond promptly, and no later than the timeframes prescribed by applicable law, to ensure your rights are respected.

Requests relating to Guest Mode. Guest Mode sessions are not linked to your name or email address. If you submit a privacy rights request relating to a Guest Mode session, we may be unable to identify the data relating to you. In that case, we will inform you, and you may provide additional information to enable us to locate and act on your data. Where we cannot identify you even with such information, certain rights may not apply, as provided by Article 11 GDPR.

If you are located in the UK, you have the right to make a data protection complaint directly to us if you consider that our processing of your personal data infringes UK data protection law. You can do this by emailing privacy@talkpal.ai (or our Data Protection Officer at dataprivacy@kertos.io), or via our UK representative at https://app.prighter.com/portal/talkpal. We will acknowledge your complaint within 30 days of receipt, investigate it, and inform you of the outcome without undue delay.
Making a complaint to us does not affect your right to complain to the Information Commissioner's Office (ICO), the UK supervisory authority (www.ico.org.uk). If you are located in

the EEA, you also have the right to complain to your Member State's data protection authority. If you are located in Switzerland, you may contact the Federal Data Protection and Information Commissioner.

Withdrawing your consent: If we are relying on your consent to process your personal information, which may be express and/or implied consent depending on the applicable law, you have the right to withdraw your consent at any time. Withdrawing your consent will not affect the legality of any processing conducted prior to your withdrawal. You can withdraw your consent at any time by contacting us by using the contact details provided in the section "HOW CAN YOU CONTACT US ABOUT THIS NOTICE?" below or updating your preferences.

However, please note that this will not affect the lawfulness of the processing before its withdrawal nor, when applicable law allows, will it affect the processing of your personal information conducted in reliance on lawful processing grounds other than consent.

Opting out of marketing and promotional communications: You can object to or unsubscribe from our marketing and promotional communications at any time, free of charge, by clicking the unsubscribe link in any email we send, in your account settings, or by contacting us using the details provided in the section "HOW CAN YOU CONTACT US ABOUT THIS NOTICE?" below. We will act on your objection promptly, and you will be removed from the marketing lists. However, we may still communicate with you — for example, to send you service-related messages that are necessary for the administration and use of your account and subscription (including subscription renewal reminders, trial-expiry notices, price-change notices, payment-failure notices, invoices and receipts, and cancellation or termination confirmations), to respond to service requests, or for other non-marketing purposes. These service messages are not subject to the marketing unsubscribe, as some of them are required by law or by our contract with you.

Account Information

If you would at any time like to review or change the information in your account or terminate your account, you can:

- Log in to your account settings and update your user account.
- Contact us using the contact information provided.

Upon your request to terminate your account, we will deactivate or delete your account and information from our active databases. Sub-Account Deactivation vs. Account Deletion. Deactivation of an individual sub-account (for example, when an Organizational Sub-Account is removed) is not the same as termination of your entire Account. When a sub-account is deactivated, only the Sub-Account Data associated with that specific sub-account is deleted (within 30 days, as described in Section 9). Your Account and all other sub-accounts remain active. If you request deletion of your entire Account, all sub-accounts and their associated data

will be deleted in accordance with the retention periods described above. We retain your personal data for as long as your account is active and for a period of a maximum 30 days following account deletion, after which it is permanently purged from our active systems, except that certain categories are kept for shorter, category-specific periods — in particular, conversation transcripts are automatically deleted no later than thirty-six (36) months after your last activity in that conversation, even while your account remains active, as described in Section 9. Data contained in automated backups may persist for up to 90 days before being overwritten in the normal course of our backup rotation. Notwithstanding the above, we may retain certain data for longer periods where required by law. This includes financial and billing records in accordance with applicable tax and accounting obligations, and any data we are required to preserve in connection with a legal claim, regulatory investigation, or fraud prevention obligation. Aggregated or anonymized data, which cannot reasonably be used to identify you, may be retained indefinitely for product improvement and analytical purposes.

Cookies and similar technologies: Most Web browsers are set to accept cookies by default. If you prefer, you can usually choose to set your browser to remove cookies and to reject cookies. If you choose to remove cookies or reject cookies, this could affect certain features or services of our Services. However, please note that rejecting cookies may impact your experience on the Services, including certain features or functionality that rely on cookies to operate. You may also opt out of interest-based advertising by advertisers on our Services. For further information, please see our Cookie Notice: https://talkpal.ai/cookie-policy/.

If you have questions or comments about your privacy rights, you may email us at privacy@talkpal.ai.

13. CONTROLS FOR DO-NOT-TRACK FEATURES

In Short: Most web browsers and some mobile operating systems and mobile applications include a Do-Not-Track (“DNT”) feature or setting you can activate to signal your privacy preference not to have data about your online browsing activities monitored and collected. At this stage, no uniform technology standard for recognizing and implementing DNT signals has been finalized, and we do not currently respond to DNT browser signals. However, we do recognize the Global Privacy Control (“GPC”) signal as a valid opt-out-of-sale/sharing request where required by applicable law (including the CCPA/CPRA, the Colorado Privacy Act, and the other State Laws described in Section 14 that recognize universal opt-out mechanisms). If your browser or device transmits a GPC signal, we will treat it as a request to opt out of the “sharing” of your personal information for cross-context behavioral advertising as described in Section 14. You may also opt out manually by contacting us at privacy@talkpal.ai. If a standard for online tracking is adopted that we must follow in the future, or if we update our practices to align with evolving technology standards or legal requirements, we will inform you about that practice in a

revised version of this privacy notice.

14. DO UNITED STATES RESIDENTS HAVE SPECIFIC PRIVACY RIGHTS?

In Short: *If you are a resident of California, Virginia, or another U.S. state with a comprehensive consumer privacy law (listed below), you have specific rights regarding your personal information, including the right to opt out of targeted advertising.*

What categories of personal information do we collect?

We have collected the following categories of personal information in the past twelve (12) months:

Category	Examples	Collected
A. Identifiers	Contact details, such as real name, alias, telephone or mobile contact number, unique personal identifier, online identifier, Internet Protocol address, email address, and account name	YES
B. Personal information as defined in the California Customer Records statute	Name, contact information	YES
C. Protected classification characteristics under state or federal law	Gender (collected via social media logins where provided by the user or the social media platform)	YES
D. Commercial information	Transaction information, purchase history, financial details, and payment information	YES
E. Biometric information	Fingerprints and voiceprints	NO
F. Internet or other similar	Browsing history, search history, online behavior, interest data, and interactions with our and other websites, applications, systems, and advertisements	YES

network activity		
G. Geolocation data	Approximate location derived from IP address	YES
H. Audio, electronic, visual, thermal, olfactory, or similar information	Images and audio, and video or call recordings created in connection with our business activities. Audio from in-app language activities is processed transiently and not retained by Talkpal; recordings of sales, onboarding, or business calls are retained only for a limited period and then deleted.	YES
I. Professional or employment-related information	Business contact details collected when you engage with us as a business customer; or work history and professional qualifications if you apply for a job with us	YES
J. Education Information	Student records and directory information	NO
K. Inferences drawn from collected personal information	Inferences drawn from any of the collected personal information listed above to create a profile or summary about, for example, an individual's preferences and characteristics	YES
L. Sensitive personal Information		NO

Note on Category E: We process audio of user speech in real time for speech recognition and language assessment purposes (see Category H). Talkpal does not store or retain audio recordings; this audio is not processed to generate biometric identifiers such as voiceprints and is therefore not classified as biometric information under Category E. Illinois Residents: If you are an Illinois resident, we provide this additional disclosure under the Illinois Biometric Information Privacy Act (BIPA). When you use voice-based features, your speech is transmitted to third-party speech recognition providers (listed above) and processed in real time solely to provide language learning and speech assessment functionality. **Talkpal does not store or retain audio recordings of your speech.** We do not use this audio to create voiceprints or other biometric identifiers. Any temporary retention by our processing vendors is governed by our data processing agreements with them, as described in Sections 1 and 4. For questions about our audio data practices, contact us at privacy@talkpal.ai.

Biometric Data Retention and Destruction Policy (740 ILCS 14/15(a)). Talkpal provides the following written policy pursuant to Section 15(a) of the Illinois Biometric Information Privacy Act and similar laws in other jurisdictions, including the Texas Capture or Use of Biometric Identifier Act and Washington's biometric privacy statute (RCW 19.375). Talkpal does not create, collect, capture, purchase, or otherwise possess biometric identifiers or biometric information as those terms are defined under BIPA or comparable laws. Audio of your speech is transmitted in real time to our speech-processing service providers solely to generate speech recognition and language feedback; it is never stored, saved, or retained by Talkpal and exists in our systems only for the duration of the request. To the extent any data processed by Talkpal or its service providers were deemed to constitute a biometric identifier or biometric information under applicable law, such data is destroyed immediately upon completion of the real-time processing for which it was captured. Our service providers are contractually required to delete any temporarily retained audio within the limited timeframes specified in our data processing agreements, are prohibited from using it to train or improve their own models, and process it solely to provide speech recognition and language feedback on our behalf. Talkpal does not sell, lease, trade, or otherwise profit from biometric identifiers or biometric information, and does not disclose such data except to service providers acting on our documented instructions or as required by law.

Photo Mode. In Photo Mode, users practice by describing images provided by Talkpal. Users do not upload photographs or images, and Talkpal does not collect or process user-submitted images or any facial data.

Guest Mode. Personal information processed in iOS Guest Mode falls within Categories A (device identifiers, IP address), F, and G above and is handled as described in Section 1. Guest Mode does not capture your voice or any other Category H information. We do not collect Categories B, C, D, H, I, or K from Guest Mode users.

Note on Category L: We do not intentionally collect or process sensitive personal information, and we do not request it. Because our conversation modes accept free-form input, a user may voluntarily mention such information during a conversation; where that happens it is processed only as part of the immediate conversational content, as described in Section 1, and is not used to derive sensitive-data insights, for profiling, or for targeted advertising.

We will use and retain the collected personal information as needed to provide the Services or for:

- Category A, Category B, Category C, Category D, Category F, Category G, Category H, Category I, Category K – As long as the user has an account with us, plus up to 30 days following account deletion (up to 90 days in automated backups). Text transcripts of conversations with the AI tutor (Categories F, H and K) are deleted no later than 36 months after your last activity in that conversation, even while your account remains active (see

Section 9). See Sections 9 and 12 for full retention details, including extended retention for legal and regulatory obligations.

For personal information associated with an Organizational Sub-Account (as described in our Terms and Conditions), the retention period is the duration of the Organizational Sub-Account plus thirty (30) days following deactivation, rather than the duration of the user's overall Account. See Section 9 for details.

We may also collect other personal information outside of these categories through instances where you interact with us in person, online, or by phone or mail in the context of:

- Receiving help through our customer support channels;
- Participation in customer surveys or contests; and
- Facilitation in the delivery of our Services and to respond to your inquiries.

How do we use and share your personal information?

Learn about how we use your personal information in the section, "HOW DO WE PROCESS YOUR INFORMATION?"

We collect and share your personal information through:

- Targeting cookies/Marketing cookies
- Social media cookies
- Beacons/Pixels/Tags

Will your information be shared with anyone else?

We may disclose your personal information with our service providers pursuant to a written contract between us and each service provider. Learn more about how we disclose personal information to in the section, "WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?"

We may use your personal information for our own business purposes, such as for undertaking internal research for technological development and demonstration. This is not considered to be "selling" of your personal information.

We do not sell personal information for money or other valuable consideration. However, we do 'share' certain identifiers, online activity, approximate location, and inferences with advertising partners for cross-context behavioral advertising (targeted advertising) as defined under the CCPA/CPRA, which is why we offer the opt-out described below. We do not use personal

information for profiling in furtherance of decisions that produce legal or similarly significant effects concerning consumers. We have disclosed the following categories of personal information to third parties for a business or commercial purpose in the preceding twelve (12) months:

- Category A. Identifiers — shared with ad networks and analytics,
- Category D. Commercial information — shared with payment processors,
- Category F. Internet or similar network activity — shared with analytics and retargeting platforms,
- Category G. Geolocation data — shared with analytics and ad services,
- Category H. Audio, electronic, visual, or similar information — in-app language audio is shared with AI processing and speech recognition vendors and is processed transiently and not retained by Talkpal; recordings of sales, onboarding, or business calls are shared with our meeting-recording and transcription and CRM providers and retained only for a limited period,
- Category K. Inferences drawn from collected personal information.

In addition to the above disclosures for business purposes, we "share" (as defined under the CCPA/CPRA) the following categories of personal information with advertising partners for cross-context behavioral advertising:

- Category A. Identifiers — such as IP address, device identifiers, online identifiers, and hashed email addresses used for audience matching — shared with ad networks and retargeting platforms
- Category F. Internet or other similar network activity — such as browsing behavior, search history, and interactions with advertisements — shared with ad networks, analytics providers, and retargeting platforms
- Category G. Geolocation data — such as approximate location derived from IP address — shared with ad networks and analytics providers
- Category K. Inferences drawn from collected personal information — such as a modeled estimate of the expected value of a subscription, sent together with conversion events to advertising partners for campaign measurement and bidding

You have the right to opt out of this sharing. To exercise it, visit https://talkpal.ai/do-not-sell-share-my-personal-information/, enable the Global Privacy Control signal in your browser, or contact us at privacy@talkpal.ai.

The categories of third parties to whom we disclosed personal information for a business or commercial purpose can be found under “WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?”

California Residents

California Civil Code Section 1798.83, also known as the “Shine The Light” law permits our users who are California residents to request and obtain from us, once a year and free of charge, information about categories of personal information (if any) we disclosed to third parties for direct marketing purposes and the names and addresses of all third parties with which we shared personal information in the immediately preceding calendar year. If you are a California resident and would like to make such a request, please submit your request in writing to us using the contact information provided below.

Statutory disclosure regarding California minors. The Services are intended only for users who are at least 18 years old (or considered non-minor in the local jurisdiction), and we do not knowingly permit registration by, collect personal information from, or market to anyone under 18. Users represent that they meet this age requirement by accepting our Terms and Conditions at registration, and we deactivate accounts and delete associated personal information promptly upon learning that a user is under 18, as described in Section 11 of this notice. Notwithstanding the foregoing, California Business and Professions Code Section 22581 requires us to provide a removal mechanism in the event a California resident under 18 has nonetheless obtained an account contrary to our age requirement. If you are a California resident under 18 with a registered account, you (or your parent or guardian) may request removal of content you have publicly posted on the Services by emailing privacy@talkpal.ai from the email address associated with the account, including a statement that you reside in California and are under 18. Upon verification, we will remove or anonymize publicly visible content as required by law and deactivate the account in accordance with our Terms and Conditions and Section 11 of this notice. Please note that complete removal from all systems (including backups) may not be possible, but we will ensure that the content is not publicly displayed on the Services and that any retained data is handled in accordance with the retention periods described in Sections 9 and 12.

CCPA Privacy Notice

This section applies only to California residents. Under the California Consumer Privacy Act (CCPA), you have the rights listed below.

The California Code of Regulations defines a “residents” as:

(1) every individual who is in the State of California for other than a temporary or transitory purpose and

(2) every individual who is domiciled in the State of California who is outside the State of California for a temporary or transitory purpose

All other individuals are defined as “non-residents.”

If this definition of “resident” applies to you, we must adhere to certain rights and obligations regarding your personal information.

Your rights with respect to your personal data

Right to request deletion of the data — Request to delete

You can ask for the deletion of your personal information. If you ask us to delete your personal information, we will respect your request and delete your personal information, subject to certain exceptions provided by law, This includes exceptions such as (but not limited to):

- the exercise of another consumer’s right to free speech or other legal rights;
- our compliance with legal obligations, such as tax or regulatory reporting;
- internal uses that are reasonably aligned with your expectations as a consumer, such as maintaining transaction records for legitimate business purposes; or
- detecting or protecting against fraudulent, illegal, or harmful activities.

Right to be informed — Request to know

Depending on the circumstances, you have a right to know:

- whether we collect and use your personal information;
- the categories of personal information that we collect;
- the retention periods for each category of personal information, or the criteria we use to determine such periods;
- the purposes for which the collected personal information is used;
- whether we sell or share personal information to third parties;
- the categories of personal information that we sold, shared, or disclosed for a business purpose;
- the categories of third parties to whom the personal information was sold, shared, or disclosed for a business purpose;

- the business or commercial purpose for collecting, selling, or sharing personal information; and
- the specific pieces of personal information we collected about you.

In accordance with applicable law, we are not obligated to provide or delete consumer information that is de-identified in response to a consumer request or to re-identify individual data to verify a consumer request.

Right to Non-Discrimination for the Exercise of a Consumer's Privacy Rights

We will not discriminate against you if you exercise your privacy rights.

Right to Limit Use and Disclosure of Sensitive Personal Information

We do not intentionally collect or process sensitive personal information as defined under the CCPA/CPRA, and we do not use or disclose it for any purpose that would require us to offer a Right to Limit.

Verification process
Upon receiving your request, we will need to verify your identity to determine you are the same person about whom we have the information in our system. Verification is essential to protect your data and prevent unauthorized access or misuse. These verification efforts require us to ask you to provide information so that we can match it with information you have previously provided us. For instance, depending on the type of request you submit, we may:

- Ask you to provide specific details, such as your name, email address, account information, or recent transactions made through our Services.
- Contact you through a communication method (e.g., email or phone) that you have previously provided to us.
- Use multifactor authentication, such as sending a verification code to your registered email or phone number, to confirm your identity.
- Request additional documentation if necessary, such as a government-issued ID or proof of address, to validate your identity for sensitive or high-risk requests.

In some cases, we may rely on third-party identity verification services to enhance the security and efficiency of the verification process.
We will only use personal information provided in your request to verify your identity or authority to make the request. This information will not be used for any other purpose unless required by law. To the extent possible, we will avoid requesting additional information from you

for the purposes of verification. However, if we cannot verify your identity from the information already maintained by us, we may:

- Request that you provide additional information for the purposes of verifying your identity and for security or fraud-prevention purposes.
- Inform you of why the information provided was insufficient to complete the verification process and guide you on next steps.

We take your privacy seriously and have implemented strict security measures to protect any additional information provided during the verification process. We will delete such additionally provided information as soon as we finish verifying you. If we cannot complete the verification process after reasonable efforts, we may decline the request and inform you of your options, including how to appeal the decision.

Other privacy rights

- You may object to the processing of your personal information.
- You may request correction of your personal data if it is incorrect or no longer relevant, or ask to restrict the processing of the information.
- You can designate an authorized agent to make a request under the CCPA on your behalf. We may deny a request from an authorized agent that does not submit proof that they have been validly authorized to act on your behalf in accordance with the CCPA.
- You may request to opt out from future selling or sharing of your personal information to third parties. Upon receiving an opt-out request, we will act upon the request as soon as feasibly possible, but no later than fifteen (15) days from the date of the request submission.

To exercise these rights, you can contact us by email at privacy@talkpal.ai, or by referring to the contact details at the bottom of this document. If you have a complaint about how we handle your data, we would like to hear from you.

Virginia Residents

Under the Virginia Consumer Data Protection Act (VCDPA):

“Consumer” means a natural person who is a resident of the Commonwealth acting only in an individual or household context. It does not include a natural person acting in a commercial or employment context.

“Personal data” means any information that is linked or reasonably linkable to an identified or identifiable natural person. “Personal data” does not include de-identified data or publicly

available information.

“Sale of personal data” means the exchange of personal data for monetary consideration.

If this definition of “consumer” applies to you, we must adhere to certain rights and obligations regarding your personal data.

We collect, use, and share the same categories of personal data described in the California section above. For the categories of personal data we process, the purposes for processing, and the categories of third parties with whom we share personal data, please refer to the tables and disclosures in the California Residents section of this notice, which apply equally to Virginia residents. We do not sell personal data for monetary consideration. We do process personal data for targeted advertising as described above; you have the right to opt out of this processing.

Your rights with respect to your personal data

- Right to be informed whether or not we are processing your personal data
- Right to access your personal data
- Right to correct inaccuracies in your personal data
- Right to request deletion of your personal data
- Right to obtain a copy of the personal data you previously shared with us
- Right to opt out of the processing of your personal data if it is used for targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects (“profiling”)
- Right to lodge a complaint if you believe we are not processing your personal data in compliance with applicable laws, you have the right to file a complaint with a data protection authority in your jurisdiction.

Exercise your rights provided under the Virginia VCDPA

You may contact us by email at privacy@talkpal.ai, or opt out of targeted advertising at https://talkpal.ai/do-not-sell-share-my-personal-information/.

If you are using an authorized agent to exercise your rights, we may deny a request if the authorized agent does not submit proof that they have been validly authorized to act on your behalf.

Verification process

We may request that you provide additional information reasonably necessary to verify you and your consumer's request. If you submit the request through an authorized agent, we may need to collect additional information to verify your identity before processing your request. Authorized agents must provide verifiable documentation, such as a signed authorization letter or a valid power of attorney, to act on your behalf.

Upon receiving your request, we will respond without undue delay, but in all cases, within forty-five (45) days of receipt. The response period may be extended once by forty-five (45) additional days when reasonably necessary. If an extension is required, we will inform you in writing and provide a detailed explanation for the delay, as well as an expected completion date. In cases where we are unable to verify your identity with the information provided, we will notify you promptly and explain what additional steps are required to complete the verification process. If you fail to provide sufficient information for verification within a reasonable timeframe, your request may be denied, and we will inform you of the reasons for denial. We will maintain a record of verification requests and responses for legal compliance purposes, ensuring that we process all requests in accordance with applicable privacy regulations.

Right to appeal

If we decline to take action regarding your request, we will inform you of our decision and reasoning behind it. If you wish to appeal our decision, please email us at privacy@talkpal.ai. Within sixty (60) days of receipt of an appeal, we will inform you in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If your appeal is denied, you may contact the Attorney General to submit a complaint.

Other US State Residents

This subsection applies to residents of U.S. states with comprehensive consumer privacy laws that apply to Talkpal (together, the "State Laws"), including, as of the date of this notice, Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas and Utah, in each case to the extent the relevant law applies to us. Your rights depend on the State Law that applies to you and may include: the right to confirm whether we process your personal data and to access it; the right to correct inaccuracies; the right to delete personal data you provided or we obtained about you; the right to obtain a portable copy; and the right to opt out of the processing of your personal data for (i) targeted advertising, (ii) the sale of personal data, and (iii) profiling in furtherance of decisions that produce legal or similarly significant effects. Residents of Oregon and Minnesota may additionally request a list of the specific third parties, and residents of Delaware and Maryland a list of the categories of third parties, to which we have disclosed personal data. As of the date of this notice: we process identifiers, commercial

information, internet or other network activity information, and inferences for targeted advertising; we do not sell personal data for monetary consideration; and we do not engage in profiling in furtherance of decisions that produce legal or similarly significant effects.
To opt out of targeted advertising, visit https://talkpal.ai/do-not-sell-share-my-personal-information/ or enable the Global Privacy Control signal in your browser, which we honor where required by the State Laws. You may opt out of AI-model improvement directly in the app or your account settings. To exercise any other right, contact us at privacy@talkpal.ai; we will respond within the timeframe required by your State Law, and only you or an authorized agent with verifiable proof of authority may submit a request. If we decline to act on your request, we will explain why and, where your State Law provides for it, you may appeal by replying to our decision or emailing privacy@talkpal.ai with "Appeal" in the subject line. If your appeal is denied, you may contact your state's Attorney General.

For information about the categories of personal information we collect, the purposes for processing, and the categories of third parties with whom we share or disclose information, please refer to the tables and disclosures in the California Residents section of this notice, which apply to all U.S. residents.

15. DO WE MAKE UPDATES TO THIS NOTICE?

In Short: *Yes, we will update this notice as necessary to stay compliant with relevant laws.*

We may update this privacy notice from time to time. The updated version will be indicated by an updated "Last updated" date and the updated version will be effective as soon as it is accessible. For significant changes that materially affect how we process your personal information, we will provide more prominent notice, such as a banner on our website, an in-app alert, or direct communication via email or other contact methods you have provided.
In some cases, where legally required, we will seek your explicit consent before implementing changes to how we process your personal information. We encourage you to review this privacy notice frequently to be informed of how we are protecting your information. Your continued use of our Services following the posting of updated versions of this privacy notice will constitute your acknowledgment of the updates and your agreement to comply with the latest version.

This privacy notice was originally drafted in English (United States). In the event of any conflict, ambiguity, or inconsistency between the English-language version and any translated version, the English-language version shall control, except where mandatory law in your jurisdiction requires that this notice be provided in a specific language, in which case the version in that language shall apply to the extent (and only to the extent) required by such mandatory law.

16. HOW CAN YOU CONTACT US ABOUT THIS NOTICE?

If you have questions or comments about this notice, you may email us at privacy@talkpal.ai or contact us by post at:

TalkPal, Inc.
2810 N Church St,
PMB 54222,
Wilmington, DE 19802-4447,
United States

Representative
We value your privacy and your rights as a data subject and have therefore appointed Prighter Group with its local partners as our privacy representative and your point of contact for the following regions:

- United Kingdom (UK)
- European Union (EU)

Prighter gives you an easy way to exercise your privacy-related rights (e.g. requests to access or erase personal data). If you want to contact us via our representative, Prighter or make use of your data subject rights, please visit the following website:
https://app.prighter.com/portal/talkpal

Data Protection Officer
We have appointed an external Data Protection Officer in accordance with Article 37 of the GDPR. You may contact our Data Protection Officer directly with any questions or concerns regarding the processing of your personal data:
Kertos GmbH
Brienner Str. 41, 80333 Munich, Germany
Data Protection Officer: Dr. Kilian Schmidt
Email: dataprivacy@kertos.io
Phone: +49 151 525 797 93

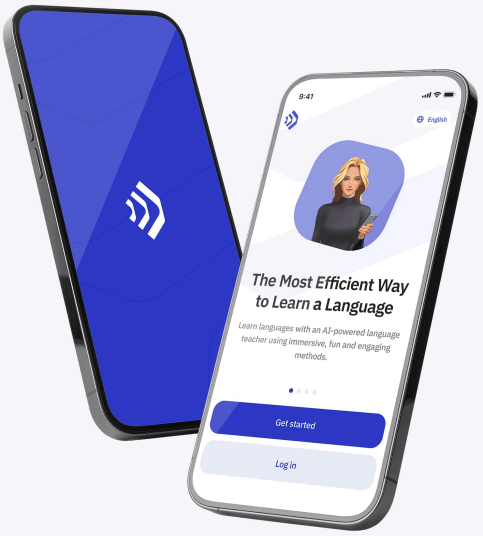
17. HOW CAN YOU REVIEW, UPDATE, OR DELETE THE DATA WE COLLECT FROM YOU?

Based on the applicable laws of your country, you may have the right to request access to the personal information we collect from you, change that information, or delete it. To request to review, update, or delete your personal information, please email us at privacy@talkpal.ai.

DOWNLOAD TALKPAL APP

LEARN ANYWHERE ANYTIME

Talkpal is an AI-powered language tutor available on web and mobile platforms. Accelerate your language fluency, chat about interesting topics by writing or speaking, and receive realistic voice messages wherever and whenever you want.



Download on the App Store

GET IT ON Google Play

GET IN TOUCH WITH US

We are always here if you have any questions or require assistance. Contact our customer support anytime at support@talkpal.ai

Languages

Learn English

Learning

Grammar

Learn Spanish
Learn French
Learn Italian
Learn German
Learn Ukrainian
Learn Dutch
Learn Swedish
Learn Finnish
Learn Arabic
Learn Chinese
Learn Hindi
Learn Japanese
Learn Korean
Learn Portuguese
119+ more Languages

Courses
Roleplays
Characters
Debates
Photo Mode
Call Mode
Sentence Mode
Word Mode
Dialogue Mode
Language Certificates
Video Lessons
Improve Listening
Improve Speaking
Improve Reading
Improve Writing

Partnerships

Talkpal for Education
Talkpal for Business
Talkpal for Enterprise
Talkpal for Nonprofits
Talkpal for Resellers & Partnerships
Talkpal Affiliate

Company

About
Blog
Press
Pricing
Contact
Help Center
Privacy Policy
Trust Center
Cookie Policy
Cookie Preference
Terms and Conditions
Safety and Crisis
Resources

End User License Agreement

Do not sell/share my personal information

Imprint

© 2026 All Rights Reserved.

Talkpal, Inc., 2810 N Church St, PMB 54222, Wilmington, Delaware 19802, US

English

Trustpilot