Privacy Policy

Keywise AI (“we,” “our,” or “us”) is committed to protecting your privacy. This Privacy Policy explains how your personal information is collected, used, and disclosed by Keywise AI.
This Privacy Policy applies to our website, and its associated subdomains (collectively, our “Service”) alongside our application, Keywise AI. By accessing or using our Service, you signify that you have read, understood, and agree to our collection, storage, use, and disclosure of your personal information as described in this Privacy Policy and our Terms of Service.

Definitions and key terms

To help explain things as clearly as possible in this Privacy Policy, every time any of these terms are referenced, are strictly defined as:

Cookie: small amount of data generated by a website and saved by your web browser. It is used to identify your browser, provide analytics, remember information about you such as your language preference or login information.

Company: when this policy mentions “Company,” “we,” “us,” or “our,” it refers to Lanker Sp z o.o. that is responsible for your information under this Privacy Policy.

Country: where Keywise AI or the owners/founders of Keywise AI are based, in this case is Poland.

Customer: refers to the company, organization or person that signs up to use the Keywise AI Service to manage the relationships with your consumers or service users.

Device: any internet connected device such as a phone, tablet, computer or any other device that can be used to visit Keywise AI and use the services.

IP address: Every device connected to the Internet is assigned a number known as an Internet protocol (IP) address. These numbers are usually assigned in geographic blocks. An IP

address can often be used to identify the location from which a device is connecting to the Internet.

Personnel: refers to those individuals who are employed by Keywise AI or are under contract to perform a service on behalf of one of the parties.

Personal Data: any information that directly, indirectly, or in connection with other information — including a personal identification number — allows for the identification or identifiability of a natural person.

Service: refers to the service provided by Keywise AI as described in the relative terms (if available) and on this platform.

Third-party service: refers to advertisers, contest sponsors, promotional and marketing partners, and others who provide our content or whose products or services we think may interest you.

You: a person or entity that is registered with Keywise AI to use the Services.

Information automatically collected

There is some information like your Internet Protocol (IP) address and/or browser and device characteristics — is collected automatically when you visit our platform. This information may be used to connect your computer to the Internet. Other information collected automatically could be a login, e-mail address, password, computer and connection information such as browser plug-in types and versions and time zone setting, operating systems and platforms, purchase history, (we sometimes aggregate with similar information from other Users), the full Uniform Resource Locator (URL) clickstream to, through and from our Website that may include date and time; cookie number; parts of the site you viewed or searched for; and the phone number you used to call our Customer Services. We may also use browser data such as cookies, Flash cookies (also known as Flash Local Shared Objects) or similar data on certain parts of our Website for fraud prevention and other purposes. During your visits, we may use software tools such as JavaScript to measure and collect session information

including page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page. We may also collect technical information to help us identify your device for fraud prevention and diagnostic purposes.
We automatically collect certain information when you visit, use or navigate the platform. 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, location, information about who and when you use our and other technical information. This information is primarily needed to maintain the security and operation of our platform, and for our internal analytics and reporting purposes.

Collection of Personal Data and Method

Keywise AI may process your personal data for the purposes specified in this Privacy Policy. The personal data of users collected and used by Keywise AI in particular, are as follows: phone number which we will receive once you contact Keywise AI, and identifier for advertisers designated in your mobile device used in accessing our services (The Identifier for Advertisers-IDFA), identifier for vendors/developers designated your mobile device (The Identifier for Vendors-IDVF) and Internet Protocol Address-IP Address).

Data Categories and Data Types

Contact Information: Phone number, e-mail address

Process Security: Internet traffic data (network movements, IP address, visit data, time and date information), device name, In-app purchase history, identifier for advertisers designated in your mobile device used in accessing our services (if you give a permission, the Identifier for Advertisers-IDFA), identifier for vendors/developers designated your mobile device (The Identifier for Vendors-IDVF)

Customer Transaction: Order information

Marketing Data: IDFA, IDVF

We may collect your above mentioned data directly from you through electronic or physical mediums, your mobile device, third party applications or third party sources which you can access our application through these mediums such as Apple App Store, Google Play App Store, Amazon App Store (similar platforms together with “App Stores”), for the purposes of compliance with legal obligations, enhancing our services, administering your use of our services, as well as enabling you to enjoy and easily navigate our services.

We may collect your Log Data generated while you are using our services/applications (through our products or third party products). This Log Data may include information such as your device’s Internet Protocol (“IP”) address, device name, operating system version, the configuration of the app when utilizing our service/application, the time/date of your use of the service/application, and other statistics.

How We Use Your Information

We use your information for a variety of business purposes, including to provide our Services, for administrative purposes, and to market our products and Services, as described below.

Provide Our Services

We use your information to fulfill our contract with you and provide you with our Services, such as:

(a) Providing responses to your text messages and search queries, and other similar Services;

(b) Managing your information and accounts;

(c) Providing access to certain areas, functionalities, and features of our Services;

(d) Answering requests for customer or technical support;

(e) Communicating with you about your account, activities on our Services, and policy changes; and

(f) Processing your financial information and other payment methods for products or Services purchased.

Administrative Purposes

We use your information for various administrative purposes, such as:

(a) Pursuing our legitimate interests such as direct marketing, research and development (including marketing research), network and information security, and fraud prevention;

(b) Detecting security incidents, protecting against malicious, deceptive, fraudulent or illegal activity, and prosecuting those responsible for that activity;

(c) Measuring interest and engagement in our Services;

(d) Short-term, transient use, such as contextual customization of ads;

(e) Improving, upgrading or enhancing our Services;

(f) Developing new features and Services;

(g) Ensuring internal quality control and safety;

(h) Authenticating and verifying individual identities;

(i) Debugging to identify and repair errors with our Services;

(j) Auditing relating to interactions, transactions and other compliance activities;

(k) Enforcing our agreements and policies; and

(l) Complying with our legal obligations.

Marketing and Advertising our Products and Services

We may use personal information to tailor and provide you with content and advertisements. We may provide you with these materials as permitted by applicable law. Some of the ways we may market to you include email campaigns, custom audiences advertising, and “interest-based” or “personalized advertising,” including through cross-device tracking.

If you have any questions about our marketing practices or if you would like to opt out of the use of your personal information for marketing purposes, you may contact us at any time as set forth in Section 15 below.

Other Purposes

We also use your information for other purposes as requested by you or as permitted by applicable law.

(a) Share Content with Friends or Colleagues. Our Services may offer various tools and functionalities. For example, we may allow

you to provide information about your friends or colleagues through our referral services. Our referral services may allow you to forward or share certain content with a friend or colleague, such as an email inviting your friend to use our Services.

How We Disclose Your Information

We disclose your information to third parties for a variety of business purposes, including to provide our Services, to protect us or others, or in the event of a major business transaction such as a merger, sale, or asset transfer, as described below.

Disclosures to Provide our Services

The categories of third parties with whom we may share your information are described below.

(a) Other Users or Third Parties: When you use the Services, you may choose to share personal information or content with other users or third parties. In addition, certain aspects of your profile may be available to other users.

(b) Service Providers: We may share your personal information with our third-party service providers who use that information to help us provide our Services. This includes service providers that provide us with IT support, hosting, payment processing, customer service, and related services.

(c) Business Partners: We may share your personal information with business partners to provide you with a product or service you have requested. We may also share your personal information to business partners with whom we jointly offer products or services.

(d) Advertising Partners: We may share your personal information, except for your biometric data, with third-party advertising partners. These third-party advertising partners may set Technologies and other tracking tools on our Services to collect information regarding your activities and your device (e.g., your IP address, cookie identifiers, page(s) visited, location, time of day). These advertising partners may use this information (and similar information collected from other services) for purposes of delivering personalized advertisements to you when you visit digital properties within

their networks. This practice is commonly referred to as “interest-based advertising” or “personalized advertising.”

(e) APIs/SDKs: We may use third-party application program interfaces (“APIs”) and software development kits (“SDKs”) as part of the functionality of our Services. For more information about our use of APIs and SDKs, please contact us as set forth below.

Disclosures to Protect Us or Others

We may access, preserve, and disclose any information we store associated with you to external parties if we, in good faith, believe doing so is required or appropriate to: comply with law enforcement or national security requests and legal process, such as a court order or subpoena; protect your, our, or others’ rights, property, or safety; enforce our policies or contracts; collect amounts owed to us; or assist with an investigation or prosecution of suspected or actual illegal activity.

Retention of Personal Information

We may store the personal information we collect as described in this Privacy Notice for as long as you use our Services or as necessary to fulfill the purpose(s) for which it was collected, provide our Services, resolve disputes, establish legal defenses, conduct audits, pursue legitimate business purposes, enforce our agreements, and comply with applicable laws.

Notwithstanding the foregoing, we may store biometric data for twenty four (24) hours.

General Principles Regarding Personal Data Processing

In accordance with this Privacy Policy, personal data are processed by Lanker sp z o.o. as a data controller in line with the basic principles named here: (i) being in accordance with law and good faith, (ii) being accurate and, where necessary, up-to- date, (iii) being processed for specific, explicit and legitimate purposes, (iv) being limited for the purpose for which they are processed and data minimization; and (v) being stored for the period stipulated in the relevant legislation or required for the purpose for which they are processed.

Purposes of Processing Personal Data and Legal Reasons

Your personal data will be processed via automatic or non-automatic means for the purposes stated below, in accordance with the applicable legislation and articles 5 and 6 of the PDP Law where it is expressly permitted by the laws, the establishment of a contract or direct relation to the execution or performance of the contract and for the legitimate interests of Lanker sp z o.o. provided that your fundamental rights and freedoms are protected.

Purposes of Processing Personal Data Identity Information

execution of activities in compliance with legislation

execution of company/product/service commitment operations

Contact Information

execution of communication activities

execution/auditing of business activities

conducting after-sales support services for goods/services

execution of goods/services sales processes

conducting storage and archive activities

execution of agreement processes

execution of information security processes

conducting audit/ethical activities

execution/audit of business activities

Process Security

conducting activities to ensure business continuity

providing information to authorized persons, institutions and organizations

execution/auditing of business activities

conducting after-sales support services for goods/services

Customer Transaction

execution of goods/services sales processes

conducting activities for customer satisfaction

execution of agreement processes

execution of activities in compliance with legislation

Visual and Audio Records

execution of agreement processes

conducting storage and archive activities

conducting marketing analysis studies

Marketing Data

execution of advertising/campaign/promotion processes

In accordance with this text, your personal data is processed for the following purposes in accordance with the above general conditions

Legal Reasons Identity Information, Contact Information, Visual and Audio Records, Customer Transaction

It is necessary to process your personal data, provided that we establish a contractual relationship with you, or that it is directly related to our performance obligation arising from this contract

We have to process data in order to establish a right for you, to exercise and protect this right

Process Security

The law explicitly stipulates the process by which we process your personal data

Conditions that are necessary in order to fulfill our legal obligation

Marketing Data

Your explicit consent Besides,
the purposes of processing personal data may be updated in line with our obligations arising from our company policies and legislation; in particular,

Creating user accounts for the service recipients/application users,

Customizing our Services, understanding our users and their preferences to enhance user experience and enjoyment using our Services and improve our users' experience,

Informing about new products, services and applications and delivering you information regarding advertisements and promotions,

Carrying out a digital subscription and In-app purchase processes of service recipients,

Carrying out the auto-renewable subscriptions for giving users access to content, services, or premium features in our service,

Carrying out the processes of information security,

Conducting activities in accordance with legislation,

Fulfilling the demands of competent authorities,

Conducting the processes of finance and accounting transactions,

Conducting communication activities,

Conducting the processes of contracts,

Carrying out strategic planning activities,

Following up requests and complaints,

Third Party Websites and Applications

Lanker sp z o.o. Apps; may contain links to other websites that are unknown to Lanker sp z o.o. and whose content is not controlled. These linked websites may contain terms and conditions other than Lanker sp z o.o. texts. Lanker sp z o.o. cannot be held responsible for the use or disclosure of information that these

websites may process. Likewise, Lanker sp z o.o. shall not have any responsibility for any links from other sites provided to the Lanker sp z o.o. Apps owned by Lanker sp z o.o.. We collect information by fair and lawful means, with your knowledge and consent. We also let you know why we're collecting it and how it will be used. You are free to refuse our request for this information, with the understanding that we may be unable to provide you with some of your desired services without it.

Push Notifications

Lanker sp z o.o. may occasionally send you push notifications via its mobile applications regarding application upgrades or notifications about our services. You can always edit such communication and notifications through the settings on your device and stop receiving such communications and notifications. Your data will be stored for the duration specified in the applicable legislation or for a reasonable time until the purpose of processing cease to exist, or during legal periods of limitation. Lanker sp z o.o. may continue to store your personal data, even after the expiry of the purpose of its use provided that it is required by other laws or a separate granted by you in this regard. In cases that you allow Lanker sp z o.o. to store your personal data for additional time by giving your consent, such data shall be immediately deleted, destructed or anonymized upon the expiry of such additional time or once the purpose of processing no longer exists.

Technical and Administrative Measures

Lanker sp z o.o. stores the personal data it processes in accordance with relevant legislation for periods stipulated in relevant legislation or required for the purpose of processing. Lanker sp z o.o. undertakes to take all necessary technical and administrative measures and to take the due care to ensure the confidentiality, integrity and security of personal data. In this context, it takes the necessary measures to prevent unlawful processing of personal data, unauthorized access to data, unlawful disclosure, modification or destruction of data. Accordingly, Lanker sp z o.o. takes the following technical and administrative measures regarding the personal data it processes:

Anti-virus application

On all computers and servers in Lanker sp z o.o.'s information technology infrastructure, a periodically updated anti-virus application is installed.

Firewall

The data center and disaster recovery centers hosting Lanker sp z o.o. servers are protected by periodically updated software-loaded firewalls; the relevant next generation firewalls control the internet connections of all staff and provide protection against viruses and similar threats during this control.

VPN

Suppliers can access Lanker sp z o.o. servers or systems through SSL-VPN defined on Firewalls. A separate SSL-VPN identification has been made for each supplier; with the identification made, the supplier only provides access to the systems that it should use or is authorized to use.

User identifications

Lanker sp z o.o. employees' authorization to Lanker sp z o.o. systems is limited only to the extent necessary by job descriptions; in case of any change of authority or duty, systemic authorizations are also updated.

Information security threat and event management

Events that occur on Lanker sp z o.o. servers and firewalls, are transferred to the "Information Security Threat and Event Management" system. This system alerts the responsible staff when a security threat occurs and allows them to respond immediately to the threat.

Encryption

Sensitive data is stored with cryptographic methods and if required, transferred through environments encrypted with cryptographic methods and cryptographic keys are stored in secure and various environments.

Logging

All transaction records regarding sensitive data are securely logged.

Two-factor authentication

Remote access to sensitive data is allowed through at least two-factor authentication.

Training

In order to increase the awareness of Lanker sp z o.o. employees against various information security violations and to minimize the impact of the human factor in information violation incidents, trainings are provided to employees at regular intervals.

Physical data security

It ensures that personal data on papers is necessarily stored in lockers and accessed only by authorized persons. Adequate security measures (for situations such as electric leakage, fire, deluge, thievery etc.) are taken based on the nature of the environment where sensitive data is stored.

Backup

Lanker sp z o.o. periodically backs up the data it stores. As a backup mechanism, it uses the backup facilities provided by the cloud infrastructure providers, as well as the backup solutions it develops when deemed necessary, provided that it is in compliance with relevant legislation and provisions of this Policy.

Non-disclosure agreement

Non-disclosure agreements are concluded with employees taking part in sensitive personal data processing.

Transfer of sensitive personal data

If transfer of sensitive personal data is required through email; such transfer is done through (i) encrypted corporate email or (ii) Registered E-mail In the event that the personal data is damaged as a result of attacks on Lanker sp z o.o. Apps or on the Lanker sp z o.o. system, despite Lanker sp z o.o. taking the necessary information security measures, or the personal data is obtained by unauthorized third parties, Lanker sp z o.o. notifies this situation to Users immediately and, if necessary, to relevant data protection authority and takes necessary measures.

Transferring Personal Data to Third Parties

The procedures and principles to be applied for transferring of personal data are regulated in articles 8 and 9 of the PDP Law, and the personal and special categories of data of the supplier may be transferred to third parties within the country or abroad since we may use servers and cloud systems located abroad. Your personal data may be transferred abroad for the following reasons

Conducting storage and archive activities

Conducting business activities

Conducting after-sales support services for goods/services

Managing customer relationship management processes

Lanker sp z o.o. may also transfer your personal data to services providers of our Company, third parties such as Facebook SDK, Adjust and Firebase Analytics which are embedded into our service for the following purposes:

Sharing identity, communication and transaction security information with authorized public institutions and organizations for the purpose of execution of activities in compliance with legislation, monitor and execution of legal affairs, informing authorized persons, institutions and organizations.

Sharing identity and contact information to manage after-sales support services, conduct business activities and manage customer relationship management processes.

Sharing identity and contact information, by user to third party applications which are integrated to the Lanker sp z o.o. Apps with the explicit consent of the User.

Personnel

If you are a Keywise AI worker or applicant, we collect information you voluntarily provide to us. We use the information collected for Human Resources purposes in order to administer benefits to workers and screen applicants.
You may contact us in order to (1) update or correct your information, (2) change your preferences with respect to communications and other information you receive from us, or (3) receive a record of the information we have relating to you. Such updates, corrections, changes and deletions will have no effect on other information that we maintain, or information that we have provided to third parties in accordance with this Privacy Policy prior to such update, correction, change or deletion.

Sale of Business

We reserve the right to transfer information to a third party in the event of a sale, merger or other transfer of all or substantially all of

the assets of Keywise AI or any of its Corporate Affiliates (as defined herein), or that portion of Keywise AI or any of its Corporate Affiliates to which the Service relates, or in the event that we discontinue our business or file a petition or have filed against us a petition in bankruptcy, reorganization or similar proceeding, provided that the third party agrees to adhere to the terms of this Privacy Policy.

Affiliates

We may disclose information (including personal information) about you to our Corporate Affiliates. For purposes of this Privacy Policy, "Corporate Affiliate" means any person or entity which directly or indirectly controls, is controlled by or is under common control with Keywise AI, whether by ownership or otherwise. Any information relating to you that we provide to our Corporate Affiliates will be treated by those Corporate Affiliates in accordance with the terms of this Privacy Policy.

Governing Law

This Privacy Policy is governed by the laws of European Union without regard to its conflict of laws provision. You consent to the exclusive jurisdiction of the courts in connection with any action or dispute arising between the parties under or in connection with this Privacy Policy except for those individuals who may have rights to make claims under Privacy Shield, or the Swiss-US framework.
The laws of European Union, excluding its conflicts of law rules, shall govern this Agreement and your use of the app. Your use of the app may also be subject to other local, state, national, or international laws.
By using Keywise AI or contacting us directly, you signify your acceptance of this Privacy Policy. If you do not agree to this Privacy Policy, you should not engage with our website, or use our services. Continued use of the website, direct engagement with us, or following the posting of changes to this Privacy Policy that do not significantly affect the use or disclosure of your personal information will mean that you accept those changes.

Your Consent

We've updated our Privacy Policy to provide you with complete transparency into what is being set when you visit our site and how it's being used. By using our app, registering an account, or

making a purchase, you hereby consent to our Privacy Policy and agree to its terms.

Links to Other Websites

This Privacy Policy applies only to the Services. The Services may contain links to other websites not operated or controlled by Keywise AI. We are not responsible for the content, accuracy or opinions expressed in such websites, and such websites are not investigated, monitored or checked for accuracy or completeness by us. Please remember that when you use a link to go from the Services to another website, our Privacy Policy is no longer in effect. Your browsing and interaction on any other website, including those that have a link on our platform, is subject to that website's own rules and policies. Such third parties may use their own cookies or other methods to collect information about you.

Advertising

This app may contain third party advertisements and links to third party sites. Keywise AI does not make any representation as to the accuracy or suitability of any of the information contained in those advertisements or sites and does not accept any responsibility or liability for the conduct or content of those advertisements and sites and the offerings made by the third parties.
Advertising keeps Keywise AI and many of the websites and services you use free of charge. We work hard to make sure that ads are safe, unobtrusive, and as relevant as possible.
Third party advertisements and links to other sites where goods or services are advertised are not endorsements or recommendations by Keywise AI of the third party sites, goods or services. Keywise AI takes no responsibility for the content of any of the ads, promises made, or the quality/reliability of the products or services offered in all advertisements.

Cookies for Advertising

These cookies collect information over time about your online activity on the app and other online services to make online advertisements more relevant and effective to you. This is known as interest-based advertising. They also perform functions like preventing the same ad from continuously reappearing and ensuring that ads are properly displayed for advertisers. Without cookies, it's really hard for an advertiser to reach its audience, or to

know how many ads were shown and how many clicks they received.

Cookies

Keywise AI uses "Cookies" to identify the areas of our website that you have visited. A Cookie is a small piece of data stored on your computer or mobile device by your web browser. We use Cookies to enhance the performance and functionality of our app but are non-essential to their use. However, without these cookies, certain functionality like videos may become unavailable or you would be required to enter your login details every time you visit the app as we would not be able to remember that you had logged in previously. Most web browsers can be set to disable the use of Cookies. However, if you disable Cookies, you may not be able to access functionality on our website correctly or at all. We never place Personally Identifiable Information in Cookies.

Blocking and disabling cookies and similar technologies

Wherever you're located you may also set your browser to block cookies and similar technologies, but this action may block our essential cookies and prevent our website from functioning properly, and you may not be able to fully utilize all of its features and services. You should also be aware that you may also lose some saved information (e.g. saved login details, site preferences) if you block cookies on your browser. Different browsers make different controls available to you. Disabling a cookie or category of cookie does not delete the cookie from your browser, you will need to do this yourself from within your browser, you should visit your browser's help menu for more information.

Payment Details

In respect to any credit card or other payment processing details you have provided us, we commit that this confidential information will be stored in the most secure manner possible.

Kids' Privacy

We do not address anyone under the age of 13. We do not knowingly collect personally identifiable information from anyone under the age of 13. If You are a parent or guardian and You are aware that Your child has provided Us with Personal Data, please

contact Us. If We become aware that We have collected Personal Data from anyone under the age of 13 without verification of parental consent, We take steps to remove that information from Our servers.

Disclaimer

Keywise AI uses OpenAI's GPT3.5 and GPT4.0 API, but we are not associated with OpenAI. We only use their official API for our app. Keywise AI is not affiliated with any government or political entity. The information provided in Keywise AI is for informational purposes only and should not be considered official or authoritative.

Changes To Our Privacy Policy

We may change our Service and policies, and we may need to make changes to this Privacy Policy so that they accurately reflect our Service and policies. Unless otherwise required by law, we will notify you (for example, through our Service) before we make changes to this Privacy Policy and give you an opportunity to review them before they go into effect. Then, if you continue to use the Service, you will be bound by the updated Privacy Policy. If you do not want to agree to this or any updated Privacy Policy, you can delete your account.

Third-Party Services

We may display, include or make available third-party content (including data, information, applications and other products services) or provide links to third-party websites or services ("Third-Party Services").

You acknowledge and agree that Keywise AI shall not be responsible for any Third-Party Services, including their accuracy, completeness, timeliness, validity, copyright compliance, legality, decency, quality or any other aspect thereof. Keywise AI does not assume and shall not have any liability or responsibility to you or any other person or entity for any Third-Party Services.

Third-Party Services and links thereto are provided solely as a convenience to you and you access and use them entirely at your own risk and subject to such third parties' terms and conditions.

Tracking Technologies

Local Storage

Local Storage sometimes known as DOM storage, provides web apps with methods and protocols for storing client-side data. Web storage supports persistent data storage, similar to cookies but with a greatly enhanced capacity and no information stored in the HTTP request header.

Information Collected Through Microsoft Clarity

Types of Data Processed: Our application uses Microsoft Clarity to process data related to user interactions on our platform. This includes, but is not limited to, mouse movements, clicks, and scrolling behavior.
Handling of Sensitive Data: We do not use Microsoft Clarity to process sensitive personal data or information related to health, financial services, or government-issued identifications.
Data Security and Protection: We take data security seriously and implement appropriate measures to protect your data. Microsoft Clarity also ensures the security and confidentiality of the data collected.
Use of Data: The data collected through Microsoft Clarity is used to analyze and improve user experience on our platform. Microsoft may use this data in accordance with its privacy policies to enhance its services.
User Rights: You have the right to access, rectify, or erase your personal data collected through Microsoft Clarity. Please contact us if you wish to exercise these rights.
Changes to our Use of Microsoft Clarity: If there are any changes to how we use Microsoft Clarity, including any additional data collection or changes in purpose, we will update this policy and notify you as required by law.

Information about General Data Protection Regulation (GDPR)

We may be collecting and using information from you if you are from the European Economic Area (EEA), and in this section of our Privacy Policy we are going to explain exactly how and why is this

data collected, and how we maintain this data under protection from being replicated or used in the wrong way.

What is GDPR?

GDPR is an EU-wide privacy and data protection law that regulates how EU residents' data is protected by companies and enhances the control the EU residents have, over their personal data.
The GDPR is relevant to any globally operating company and not just the EU-based businesses and EU residents. Our customers' data is important irrespective of where they are located, which is why we have implemented GDPR controls as our baseline standard for all our operations worldwide.

What is personal data?

Any data that relates to an identifiable or identified individual. GDPR covers a broad spectrum of information that could be used on its own, or in combination with other pieces of information, to identify a person. Personal data extends beyond a person's name or email address. Some examples include financial information, political opinions, genetic data, biometric data, IP addresses, physical address, sexual orientation, and ethnicity.
The Data Protection Principles include requirements such as:

Personal data collected must be processed in a fair, legal, and transparent way and should only be used in a way that a person would reasonably expect.

Personal data should only be collected to fulfil a specific purpose and it should only be used for that purpose. Organizations must specify why they need the personal data when they collect it.

Personal data should be held no longer than necessary to fulfil its purpose.

People covered by the GDPR have the right to access their own personal data. They can also request a copy of their data, and that their data be updated, deleted, restricted, or moved to another organization.

Why is GDPR important?

GDPR adds some new requirements regarding how companies should protect individuals' personal data that they collect and

process. It also raises the stakes for compliance by increasing enforcement and imposing greater fines for breach. Beyond these facts it's simply the right thing to do. At Keywise AI we strongly believe that your data privacy is very important and we already have solid security and privacy practices in place that go beyond the requirements of this new regulation.

Individual Data Subject's Rights - Data Access, Portability and Deletion

We are committed to helping our customers meet the data subject rights requirements of GDPR. Keywise AI processes or stores all personal data in fully vetted, DPA compliant vendors. We do store all conversation and personal data for up to 6 years unless your account is deleted. In which case, we dispose of all data in accordance with our Terms of Service and Privacy Policy, but we will not hold it longer than 60 days.

We are aware that if you are working with EU customers, you need to be able to provide them with the ability to access, update, retrieve and remove personal data. We got you! We've been set up as self service from the start and have always given you access to your data and your customers data. Our customer support team is here for you to answer any questions you might have about working with the API.

California Residents

The California Consumer Privacy Act (CCPA) requires us to disclose categories of Personal Information we collect and how we use it, the categories of sources from whom we collect Personal Information, and the third parties with whom we share it, which we have explained above.

We are also required to communicate information about rights California residents have under California law. You may exercise the following rights:

> Right to Know and Access. You may submit a verifiable request for information regarding the: (1) categories of Personal Information we collect, use, or share; (2) purposes for which categories of Personal Information are collected or used by us; (3) categories of sources from which we collect Personal Information; and (4) specific pieces of Personal Information we have collected about you.

Right to Equal Service. We will not discriminate against you if you exercise your privacy rights.

Right to Delete. You may submit a verifiable request to close your account and we will delete Personal Information about you that we have collected.

Request that a business that sells a consumer's personal data, not sell the consumer's personal data.

If you make a request, we have one month to respond to you. If you would like to exercise any of these rights, please contact us.
We do not sell the Personal Information of our users.
For more information about these rights, please contact us.

California Online Privacy Protection Act (CalOPPA)

CalOPPA requires us to disclose categories of Personal Information we collect and how we use it, the categories of sources from whom we collect Personal Information, and the third parties with whom we share it, which we have explained above.
CalOPPA users have the following rights:

Right to Know and Access. You may submit a verifiable request for information regarding the: (1) categories of Personal Information we collect, use, or share; (2) purposes for which categories of Personal Information are collected or used by us; (3) categories of sources from which we collect Personal Information; and (4) specific pieces of Personal Information we have collected about you.

Right to Equal Service. We will not discriminate against you if you exercise your privacy rights.

Right to Delete. You may submit a verifiable request to close your account and we will delete Personal Information about you that we have collected.

Right to request that a business that sells a consumer's personal data, not sell the consumer's personal data.

If you make a request, we have one month to respond to you. If you would like to exercise any of these rights, please contact us.
We do not sell the Personal Information of our users.

Keywise AI is a keyboard officially built on Open AI's ChatGPT API, and its answers are generated using artificial intelligence and machine learning algorithms. Thus, it should not be considered professional advice or expert guidance. Our company does not accept liability for any information or error in the responses provided by the chatbot. While we strive to provide accurate and helpful answers, we do not guarantee the information's accuracy, completeness, or reliability. Please be aware that our company cannot be held responsible for any damages or losses that may occur due to using the information provided by Keywise AI. Users are advised to use their discretion and judgment when relying on the provided answers.
For more information about these rights, please contact us.

Contact Us

Don't hesitate to contact us if you have any questions.

Via Email: s@hopin.it

Updated at 08-03-2024