PRIVACY POLICY

LAST UPDATED: June 30th, 2025

ABOUT US

Our Platforms ("**Platforms**" means the website(s), including but not limited to https://www.kadam.net/, https://pub.kadam.net, https://partners.kadam.net/ and related websites and/or subdomains (the "**Site**", "**Website**") and any related documentation, services; any images, logos, photographs and video content, software, designs, graphics, photos, illustrations, animations, videos, scripts, texts, music, sounds, voiceover, interactive features, and all other materials and content accessible within the Site that are incorporated into and form part of our Site and etc. ("**Site Content**")) are provided by the Company.

Company shall mean:

KADAM CY LTD, company incorporated and acting under the laws of the Republic of Cyprus under the registration number HE 424427, address: Omonoias, 13, 3052, Limassol, Cyprus (hereinafter - "**We**", "**Company**", "**Kadam"**).

We can be contacted by writing to:

Omonoias, 13, 3052, Limassol, Cyprus or via email: support@kadam.net.

The Service may also be provided to you by our partners:

Kadam Advertising Ltd, company incorporated and acting under the laws of the Republic of Cyprus under the registration number HE 441056, address: Omonoias, 13, 3052, Limassol, Cyprus.

Kadam is a large advertising network, leveraging cutting-edge technologies to deliver comprehensive solutions for advertisers and affiliates. We excel in optimizing performance, expanding reach, and fostering impactful partnerships across diverse verticals. Our innovative approach ensures enhanced engagement, higher conversions, and a seamless experience for all participants in the dynamic landscape.

We believe in the remarkable potential of technology to drive positive change and are committed to the highest standards of privacy and security. As trusted keepers of your personal data, we prioritize transparency and accountability in our data practices, ensuring that you have full knowledge of your data while benefiting from our Platforms.

When you use Platforms, we may collect, store and process some data, including personal data. This privacy policy ("**Privacy Policy**") sets out the main principles on which the data collected from you, or that you provide to us, will be processed by us. This Privacy Policy also

aims to remind you about your rights and to provide you with all the elements you need to exercise them. In accordance with data protection legislation (GDPR, UK GDPR, CCPA and etc.), we act as the controller of your personal data. In some cases, we may act as the processor of personal data, as indicated in this policy below.

We encourage you to review our Privacy Policy in its entirety to gain insight into our data handling practices. We have meticulously crafted this policy to be clear and accessible, but if you have any questions or concerns, please don't hesitate to contact us via support@kadam.net or the address below for further information:

KADAM CY LTD

Omonoias, 13, 3052, Limassol, Cyprus.

IF YOU DO NOT ACCEPT THE TERMS OF THE PRIVACY POLICY, PLEASE DO NOT USE OUR PLATFORMS.

YOUR DATA COLLECTED BY US

As you engage with our Platforms, we gather data concerning a recognized or identifiable living individual ("personal data") through the following means:

Data Directly Provided by You: this encompasses any information you manually input or furnish to us while utilizing our Platforms. For instance, this might include details like your name, email address, phone number, photo, geolocation data, place names and addresses, added by you or any other information you decide to disclose during registration or account setup as specified hereinbelow.

Data Automatically Collected by Us: when you access our Platforms, we automatically procure certain details regarding your engagement and activities within the Platforms. This may entail specifics about your device, such as its model, operating system, unique identifiers, IP address, and data related to your actions within the Platforms as specified hereinbelow.

Data Acquired via Cookies: to understand your interactions with our Platforms better, we utilize cookies and similar technologies. Cookies enable us to retain particular details about you, such as your preferences or previous interactions, thereby enhancing your experience on our Platforms and delivering tailored content. You can find more in our Cookie Policy.

INFORMATION WE COLLECT WHEN YOU CREATE AN ACCOUNT ON OUR SITE

If you have filled out the registration form and successfully registered on any of the Company’s Site, you become a User.

OUR APPROACH TO HANDLING USERS' PERSONAL DATA

User definition. A User is a person or entity that registers on the Site to access the Company's Services, including the publishing of advertising content and/or the provision of information resources for the placement of such content, aimed at reaching specific audience categories (hereinafter referred to as "Services").

Users' personal data we collect. The Company collects and processes the following Users' personal data:

- Name and surname;
- e-mail address;
- Password;
- phone number;
- Skype login;
- Telegram number;
- address of residence (street number, street, apartment, city, country, zip code)
- full User IP address;
- browser type and version;
- operating system type and version;
- information about websites visited;
- information on advertising content displayed to User on the Site;
- clicking on advertising content on the Site.

Purposes for the collection of Users' personal data. The Company collects and processes User's personal data for such purposes as:

- calculating and paying VAT and for correct accounting and billing;
- addressing the User by name;
- communication with the User;
- fast and easy User authorization on the Site;
- providing support with authorization, account management, account security, system software errors, services, bans, etc.;
- determination of the User's country of location in order to understand the scale of distribution of Services;
- executing the agreement between the Company and the User;
- preventing fraud related to the provision of Services or the use of Company systems;
- sending the most relevant advertising content regarding current Services to the User;
- analyzing the quality of Services and forecasting the Users' needs;
- corporate marketing development.

Storage of Users' personal data. The Company stores the Users' personal data for the entire period of use of the Company's Services, and no longer than 12 months from the User's last activity on the Website or until it is no longer necessary for the purposes for which it was collected, whichever comes first.

Controller of Users' personal data. During the collection of Users' personal data, the Company acts as the Controller of personal data, which means that the Company unilaterally defines the purposes and methods of processing personal data processing (hereinafter referred to as "the Controller").

Collection of missing data. Following the adoption of this updated Policy, Users who registered prior to its effective date will be required to submit the additional personal data specified herein. The provision of such data shall be a prerequisite for receiving any subsequent payments, including the first payment following the entry into force of the amended Policy.

OUR APPROACH TO HANDLING VISITORS' PERSONAL DATA

Visitor definition. A Visitor is any individual who accesses or browses the Website without registering for or using the Company's Services. Visitors do not engage with the Services provided by the Company. To access the Services, a Visitor must complete the registration process and become a User.

Visitors' personal data we collect. The Company collects and processes such Visitor personal data as:

- browser type and version;
- operating system type and version;
- information about websites visited;
- information on advertising content displayed to Visitor on the Website;
- clicking on advertising content on the Website.

Purposes for the collection of Visitors' personal data. The Company collects and processes Visitors' personal data for such purposes as:

- providing the Company's Services;
- determining the Visitor's country of location in order to understand the scale of distribution of Services;
- preventing fraud related to the provision of Services or the use of Company systems;
- sending the most relevant advertising content regarding current Services to the Visitor;
- corporate marketing development.

Storage of Visitors' personal data. The Company stores the Visitor's personal data no longer than 12 months from the last visit by the Website Visitor or until it is no longer necessary for the purposes for which it was collected, whichever comes first.

Controller of Visitors' personal data. During the collection of Visitors' personal data, the Company acts as the Controller of personal data.

OUR APPROACH TO HANDLING TRAFFIC CLIENTS' PERSONAL DATA

Traffic Client definition. A traffic Client is a data subject whose personal data is received by the Company from its counterparty (e.g. publishers) after the data subject has followed a hyperlink placed on the counterparty's website.

Traffic Clients' personal data we received. As part of their cooperation with the Company, counterparties may transfer to the Company such Traffic Client personal data as:

- unique Traffic Client's identifier in the counterparty's corporate system;
- full IP address;
- data related to the IP address (source, website, time, campaign, provider);
- data related to the browser (type, features, version, language, status, tab size);
- data related to clicks (date, time, location, characteristics, URL, ID);
- device charging data (charging & discharging time, level, status);
- data related to the device's technical specifications (vendor, model, type, OS, engine, graphic card, number of cores);
- data related to the internet connection;
- data related to location and time (time zone, city, country);
- data related to notifications (push notifications, connection type);
- data related to the screen (ratio, resolution, orientation, intervals, webview presence);
- data related to the user agent (presence, type, name, vendor, version, model, change data);
- data related to the detection of fraudulent operating systems.

Purposes for the collection of Traffic Clients' personal data. The Company collects and processes Traffic Clients' personal data for such purposes as:

- to deliver advertising content on behalf of the Company's clients;
- to measure and analyze the effectiveness of advertising campaigns, including user engagement, conversions, and other performance indicators;
- to prevent fraudulent activity, including the detection of fake traffic, invalid clicks, unauthorized automated behavior, or misuse of the Company's Services;
- to improve and develop the Company's Services, including the enhancement of targeting algorithms and ad delivery systems;
- to comply with contractual obligations to the Company's counterparties and clients, including reporting and billing based on Traffic Client interactions;
- to maintain the technical functionality and security of the advertising platform and ensure proper integration with counterparties' systems;
- to generate aggregated and anonymized statistics for internal analytics, reporting, and research purposes, without identifying any individual Traffic Client.

Storage of Traffic Clients' personal data. The Company stores the Traffic Clients' personal data no longer than 12 months from the moment the counterparty provides this data or until it is no longer necessary for the purposes for which it was collected, whichever comes first.

Traffic Clients' personal data transfer. The Company may share certain categories of Traffic Clients' personal data with counterparties strictly for the purpose of analyzing and assessing the performance, quality, and characteristics of Internet traffic related to their advertising campaigns. Such data is shared based on the Company's legitimate interest in providing its Services effectively and in accordance with contractual obligations to its partners. Where required, data sharing may also rely on the consent obtained by the Company's counterparties.

The Company may also share such data with other authorized contractors (e.g., fraud detection providers, analytics partners, or technical service providers) solely to the extent necessary for the provision and improvement of the Services, and subject to appropriate contractual safeguards, including data processing agreements as required under Article 28 GDPR.

The Company receives Traffic Clients' full IP addresses and, for real-time service operation purposes, may transmit them to selected service providers under strict confidentiality and data protection obligations. Following transmission, IP addresses are truncated and hashed by the Company and retained only in this anonymized form for security and analytics purposes.

Where personal data is transferred outside the European Economic Area (EEA), such transfers are carried out in accordance with Chapter V of the GDPR, including the use of Standard Contractual Clauses or other appropriate safeguards.

Shared Responsibility Framework for Traffic Clients' Personal Data. With respect to the collection and subsequent processing of Traffic Clients' personal data, the Company and its counterparties (including publishers) act as Joint Controllers in the meaning of Article 26 of the General Data Protection Regulation (GDPR), as they jointly determine the purposes and means of such processing.

Each counterparty (including but not limited to publishers) is solely and fully responsible for ensuring that:

- it lawfully collects Traffic Clients' personal data and obtains all necessary, valid, freely given, specific, informed, and unambiguous consent from each data subject prior to any transfer of their personal data to the Company;

- such consent expressly includes the authorization to share the personal data with the Company for the purposes described in this Policy and for subsequent processing and transfer by the Company to its partners, including advertisers, service providers, and other authorized third parties;

- the data subjects are adequately informed, in accordance with Articles 13 and 14 of the GDPR, about the identity of the Joint Controllers, the nature and purpose of the

processing, and their data protection rights.

Under no circumstances may the counterparty transmit any personal data of a Traffic Client to the Company without having obtained valid consent as described above.

The counterparty expressly acknowledges and agrees that:

- it shall bear full and sole responsibility for any failure to obtain proper consent prior to the data transfer;

- it shall indemnify and hold harmless the Company from and against any and all claims, complaints, investigations, regulatory actions, penalties, losses, damages, liabilities, costs, and expenses (including reasonable legal fees) arising out of or related to the counterparty's failure to comply with its obligations under this section;

- in the event of any third-party claim, regulatory inquiry, or legal proceeding concerning the personal data of Traffic Clients provided without valid consent, the counterparty shall, at its own cost and without limitation, defend the Company and shall assume full responsibility for any resulting damages or sanctions, including administrative fines imposed under Article 83 of the GDPR.

Each counterparty acknowledges and agrees that it must promptly notify the Company if any Traffic Client withdraws their consent for the collection, processing, or transfer of their personal data. Upon such notification, the counterparty shall cooperate fully with the Company to ensure that the Traffic Client's personal data is no longer processed or transferred in violation of their withdrawn consent. The counterparty assumes full responsibility for any failure to inform the Company in a timely manner of such withdrawal, and shall indemnify and hold harmless the Company against any claims, penalties, or damages arising from the processing of personal data contrary to the Traffic Client's revoked consent.

The Company reserves the right to suspend or terminate cooperation with any counterparty that fails to comply with the requirements set forth in this section.

Disclaimer. The Company does not represent, guarantee, or bear liability for the lawfulness of collecting, processing, using, storing, and other activities related to the personal data of parties who access/were redirected to the Website via a link that was not placed either on the Website or any other resource of the Company.

OUR APPROACH TO HANDLING COUNTERPARTIES' PERSONAL DATA

Counterparty definition. Counterparty may refer to:

- Publishers;
- SSP Platforms;
- Advertisers, including DSP Platforms that are legal entities and business contractors of the Company and which may receive Traffic Clients' data that has been

anonymized and encrypted via irreversible hashing in order to fulfill the obligations under the Company's agreement with this Platform after sending an appropriate request;
- Other contractors involved by the Company to provide Services.

Counterparties' personal data we collect. The Company collects and processes the following counterparties' personal data (including those of their employees):

- name and surname;
- person's position (if applicable);
- e-mail address;
- password;
- means of communication;
- address of residence (street number, street, apartment, city, country, zip code).

Purposes for the collection of Counterparties' personal data. The Company receives and processes contractors personal data for such purposes as:

- conducting communications regarding the execution of contracts or other financial/legal matters;
- sending advertising offers regarding Services;
- other business purposes specified in the agreement between the Company and contractor;
- corporate marketing development.

Storage of Counterparties' personal data. The Company stores the Counterparties' personal data no longer than 6 years from the termination of the agreement with that specific counterparty.

Controller of Counterparties' personal data. During the collection of Counterparties' personal data, the Company acts as the Controller of personal data.

SHARING OF YOUR PERSONAL DATA WITH THIRD-PARTY PROCESSORS

We may need to share your personal data with certain third parties as follows:

Third-party service providers:

This may include providers of certain systems and services that we use to host, administer, and maintain our Platforms, including the servers used to host our Platforms, email service providers, payment processors, fraud prevention vendors, analytics, customer service providers, providers of verification process services and other service providers.

Third-party service providers for marketing purposes:

If you consent to receive any marketing from us, certain personal data may be shared with third-party service providers we use to help us carry out marketing including, e.g., third-party marketing automation platforms.

Compliance with Laws:

We may disclose your personal data to a third party if:

a) we believe that disclosure is reasonably necessary to comply with any applicable law, regulation, legal process, or governmental request; or

b) to protect the security or integrity of the Platforms; or

c) to protect us, our customers or the public from harm or illegal activities; or

d) to respond to an emergency which we believe in the good faith requires us to disclose information to assist in preventing the death or serious bodily injury of any person.

Aggregated or Anonymized Data:

We may also share aggregated or anonymized information with third parties that do not directly identify you.

Group companies:

Your personal data may be shared among affiliates and subsidiaries. In such cases, these companies must abide by our data privacy and security requirements and are not allowed to use personal data they receive from us for any other purpose. We may also disclose personal data as part of a corporate transaction, such as a merger or sale of assets.

THE FOLLOWING ARE A FEW OF THE ESSENTIAL PROCESSORS WE TRUST:

Processor's name	Processor's privacy policy	Purpose
Intercom	https://www.intercom.com/legal/privacy	Obtain real-time customer interaction, providing instant support and engagement.
Wootric	https://inmoment.com/privacy-policy/	Collect user feedback.
UniConsent	https://www.uniconsent.com/privacy	Receive a GDPR-compliant cookie banner for the Site.
Google tag manager	https://policies.google.com/privacy	Launch and track Google ads.
Sumsub	https://sumsub.com/privacy-notice-service/	Verification of your identity.

SendGrid	https://www.twilio.com/en-us/legal/privacy	Email delivery service used for sending transactional and marketing emails, ensuring reliable communication with users.
HubSpot	https://legal.hubspot.com/privacy-policy	Transmit and store an email, login, registration date data to build a communication funnel with users.

DATA STORAGE AND CROSS-BORDER TRANSFERS

The personal data we maintain will primarily be stored and processed within the EU. We will do our best to keep this personal data secure. All information we hold is stored on our secure servers (which we own or license from appropriate third parties). We use industry-standard procedures and security standards to prevent unauthorized access to our servers.

However, there may arise situations where we need to collaborate with trusted third parties located outside the EU to deliver services to you (for instance, when utilizing servers in the US). We choose our processors very carefully. We do not work with processors based in countries where we are concerned about the rule of law with respect to privacy.

We have entered into Standard Contractual Clauses with all non-EEA third parties whose data processing tools we use (data processors) if there is no adequacy decision by the EU Commission for their particular country. We adhere to the principles of minimization and anonymization, where feasible, to ensure compliance with the GDPR and other relevant data privacy laws when transferring personal data, if necessary.

Where applicable, we rely on Standard Contractual Clauses (SCCs), adequacy decisions, or other appropriate safeguards. Consent may be requested only where no other mechanism is feasible.

CDD PROCEDURE

As stated in the Kadam User Agreement, from time to time we may require you to undergo “Customer Due Diligence" (hereinafter referred to as - “CDD”). You understand and agree that your personal data will be processed by a third party - Sumsub Group of Companies (hereinafter referred to as the “Service Provider”), in order to verify your identity for the CDD procedure, in order to comply with applicable laws, age restrictions and/or other laws and regulations.

By accepting this privacy policy, you understand and expressly, voluntarily, unambiguously and informedly agree that in the event of the CDD procedure, your personal data, including biometric information, will be processed for the purposes specified in this clause by the Service Provider, who is obliged to apply appropriate technical and organizational measures to ensure the security of your personal data to achieve the purpose of processing.

For a more detailed examination of the verification process, please refer to the Sumsub Privacy Notice.

KADAM'S PIXEL

Kadam's pixel ("pixel") offers its clients and business partners a small piece of JavaScript code that may be added to the advertisers' website in order to retarget the particular group of website users to optimize advertising on the basis of their interest in a particular ad. The pixel was designed to respect the website visitor's privacy and choices: the website does not need to collect or send the website visitor's name or contact information to Kadam, its business partner or client. The pixel is an option offered to advertisers, and the advertiser may refuse to use the pixel and use other targeting criteria instead.

Legal basis and visitor rights. Where a website visitor is situated in the EU or EEA country, the client or business partner must ensure that:

(i) website visitors are informed on the use of ad tag or pixel and their rights with respect to these technologies, and

(ii) their consent is obtained prior to collecting their personal data for advertising and marketing purposes and, particularly for retargeting, where applicable.

The business partner must either inform and/or require their partner(s) to inform the website visitors about the use of retargeting and their rights with respect to the processing of their data. An individual can opt-out of interest-based advertising using Kadam's opt-out tool, deleting the cookies via their web browser's settings or the website cookies.

Data access. The data collected is processed and stored within Kadam's systems. Neither clients (such as users or advertisers) nor our pixel licensees receive access to the raw personal data collected via the advertiser's pixel or collected via the ad tag and provided by the user. Kadam solely organizes the collection and use of personal data for retargeting to facilitate access to data subjects' rights and provide a smooth advertising service. Where more than one business partner or publisher uses our pixel to retarget one individual, Kadam does not provide such partners or publishers with access to the whole information it keeps, but only helps them optimize ads for people that expressed consent with advertising on such publisher's website.

Purposes. We use data collected by the Users and sent to the Company to enable the business partner or publisher to use our advertising services to better reach people who visit partners' websites, to optimize their ads and to measure their effectiveness (gain reports about the results from the ads) or to cap the frequency with which a website visitor receives certain advertisements. We can occasionally use this information to improve our service to serve more relevant ads to people, subject to confidentiality obligations imposed on our product service team. We may collect any information on the website user's device (such as its properties, OS, battery, version of browser etc.) to prevent fraud and gather accurate statistics on the ad efficiency.

Responsibility. The client or business partner bears full and sole responsibility for:

(i) Ensuring that website visitors are properly informed about the use of ad tags, pixels, and any related technologies on the website, as well as their rights regarding the processing of personal data for advertising and marketing purposes, including retargeting;

(ii) Securing valid, prior consent from website visitors for the collection and use of their personal data for advertising and marketing purposes, particularly for retargeting, in compliance with applicable data protection laws (e.g., GDPR in the EU/EEA).

The client or business partner must take all necessary steps to ensure compliance, including implementing appropriate mechanisms to inform visitors and collect consent, and, where applicable, ensuring that their partners or sub-contractors fulfill these obligations.

Indemnity. Clients and business partners shall defend, indemnify, and hold harmless Kadam, its affiliates, officers, directors, employees, contractors and agents from and against any and all claims, damages, liabilities, losses, costs, or expenses (including reasonable attorneys' fees) arising out of or in connection with:

(i) Non-compliance with Privacy Laws: Any failure by the client or business partner to comply with applicable data protection laws, regulations, or directives (including, but not limited to, GDPR or equivalent local legislation), particularly with regard to the requirements to:

- Inform website visitors of the use of pixels, ad tags, or similar technologies and their associated rights.
- Obtain valid, prior consent from website visitors for the collection, use, or processing of personal data for advertising or marketing purposes.

(ii) Misuse of Pixel Technology: Any unauthorized or improper use of Kadam's pixel or associated technologies by the client, business partner, or their agents, including but not limited to:

- Deploying the pixel in a manner that violates Kadam's guidelines or applicable laws.
- Collecting or transmitting personal data without appropriate consents or for purposes beyond those authorized by the visitor.

(iii) Third-party Actions: Any claim, action, or proceeding brought by third parties, including but not limited to:

- Website visitors asserting violations of their rights due to the client's or business partner's failure to comply with legal requirements.
- Business partners or advertisers failing to adhere to their contractual or legal obligations in connection with the use of Kadam's pixel.

(iv) Breach of Responsibilities: Any breach of the responsibilities outlined hereinabove, including the obligations to:

- Properly inform and secure consent from website visitors.
- Ensure that any subcontractors, partners, or third parties involved in the advertising process adhere to the same standards.

This indemnity obligation shall survive the termination or expiration of the client's or business partner's agreement with Kadam. Kadam reserves the right to assume the exclusive defense and control of any matter subject to indemnification at the client's or business partner's expense.

GOOGLE POLICIES

The Company may work with Google to deliver the best advertising opportunities to its clients. Traffic Clients and other data subjects can consult Google's policies to learn more about Google's processing policies. In particular, Google may use remarketing tags (please visit How Google uses information from sites or apps that use our services to learn more about the third parties Google works with) and other advertising cookies. Please read Google's Authorized Buyers Program, Privacy Policy and Cookie Policy to learn more.

SECURITY

Ensuring the security of your data is a top priority for us. We employ robust technical and organizational measures to safeguard the personal information entrusted to us.

Your personal data is safeguarded by the password you create when registering on our Platforms. It's essential to choose a strong password and keep it confidential to prevent unauthorized access. Additionally, refrain from sharing your password and ensure the security of your computer or mobile device.

We have instituted reasonable administrative, technical, and physical security measures to protect your personal data from unauthorized access, alteration, or destruction. For instance:

- We utilize SSL encryption (HTTPS) for all interactions involving personal data.
- Our databases are encrypted, and we store data on physically secure servers protected by firewalls.

In the event of a personal data breach as defined in Article 4.12 of the GDPR, we will promptly notify you. This notification will include relevant details, measures taken, and an assessment of associated risks, as required by applicable law and our Privacy Policy. We are committed to addressing breaches promptly and transparently, taking necessary actions such as logging affected users out, initiating password resets, and other appropriate measures to mitigate the breach.

To report a personal data breach or seek assistance, please contact us at support@kadam.net or dpo@kadam.net. We will address your concerns accordingly.

YOUR PRIVACY RIGHTS

We aim to ensure that you are fully informed about all your data protection rights and the methods available to exercise them. Please note that these rights may vary depending on your location:

- **Access:** you can request to receive a copy of the personal data we hold about you.
- **Rectification:** if you believe that any personal data, we are holding about you is incorrect or incomplete, you can request that we correct or supplement it. You can also correct some of this information directly from your account. Please contact us as soon as possible upon noticing any such inaccuracy or incompleteness.

- **Objection:** you can contact us to inform us that you object to the collection or use of your personal data for certain purposes.
- **Erasure:** you can request that we erase some or all of your personal data from our systems.
- **Restriction of Processing:** you can ask us to restrict or limit further processing of your personal data.
- **Portability:** you have the right to ask for a copy of your personal data in a machine-readable format. you can also request that we transmit the personal data to another entity where technically feasible.
- **Withdrawal of Consent:** if we are processing your personal data based on your consent (as indicated at the time of such data collection), you have the right to withdraw your consent at any time. Please note, however, that if you exercise this right, you may have then to provide express consent on a case-by-case basis for the use or disclosure of certain of your personal data, if such use or disclosure is necessary to enable you to utilize some or all Platforms.
- **Right to File Complaint:** you have the right to lodge a complaint about our practices with respect to your personal data with the supervisory authority of your country.

To exercise your rights, please contact us via support@kadam.net or write to us at the address specified hereinabove.

If you submit a request, we typically aim to fulfill it within one month. If additional time is needed to assist you in exercising your rights, we will inform you accordingly. We reserve the right to reject manifestly unfounded or excessive requests under the Art. 12(5) GDPR.

During the process of exercising your data protection rights, we may ask you to confirm your identity. This verification step ensures that you are entitled to access certain information and that the rights of third parties are not infringed upon. If we are unable to verify your request, we will be unable to fulfill it.

OUR POLICIES CONCERNING PEOPLE UNDER 18 YEARS OLD

If you are at least 18 years old, you are eligible to provide consent for the processing of your data. Alternatively, if you are under the required age, you can't use our services.

In the event that we learn that we have inadvertently gathered personal data from children, we will take reasonable measures to promptly erase such information from our records.

If you are a parent and learn that your child is using our Platforms without your permission, or if you have a specific question about data privacy, do not hesitate to get in touch with us via support@kadam.net.

If we become aware that information has been collected from persons under the age of 18, we reserve the right to promptly delete the account and erase all associated information, including health and sensitive data, from our servers.

HOW CAN YOU MANAGE YOUR DATA?

If you wish to access, correct, or update your personal data, you can do so at any time by contacting us via support@kadam.net.

If you would like us to delete your personal data, please write an email to our support team on the following email: support@kadam.net.

If you proceed with the deletion of your account, you will no longer have access to the account.

Please note that if you ask us to delete your account, all your statistics and other items will be lost and we may not be able to restore them in the future.

DATA PROTECTION OFFICER

You can reach the Company's Data Protection officer via email: dpo@kadam.net.

DATA BREACH NOTIFICATION

Assessment of risks. The Company takes all reasonable steps to minimize the risk of a personal data breach when processing personal data. The risk assessment the Company must perform should determine whether the risk to the rights and freedoms of the Data Subjects affected is judged to be sufficiently high to justify notifying them of the breach.

The Company's obligations if a data breach occurs. In the event of a personal data breach, the Company shall without undue delay and, where feasible, no later than 72 hours after having become aware of it, report the personal data breach to the DPA, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of Data Subjects. In addition, in the event of a personal data breach that may result in a high risk to the rights and freedoms of Data Subjects, the Company shall, without undue delay, notify the appropriate Data Subject whose personal data were breached. If measures have subsequently been taken to avoid high risk to Data Subjects to the degree that such risk is no longer likely to occur, communication with the Data Subject is not required by the GDPR. The Company documents all personal data breaches, including facts related to the personal data breach, its effects, and remedial actions taken. This documentation shall enable the DPA to verify compliance with the GDPR.

COMMUNICATION AND EMAIL NOTIFICATIONS POLICY

Types of Emails We Send. As part of providing our Services, we may send you email communications which fall under the following categories:

- **Transactional and Functional Emails.** These emails are sent on the legal basis of performance of a contract (Art. 6(1)(b) GDPR) or legitimate interests (Art. 6(1)(f) GDPR). They are necessary to:
    1) Assist you in onboarding and using our Platforms;
    2) Provide account-related support or system updates;
    3) Guide you through key steps in achieving your intended use of the Services.

Examples include:

(i) "Checklist: How to launch your first campaign";
(ii) "How to top up your balance — step-by-step instructions";
(iii) "You haven't logged in for 3 days — do you need help?"

Such communications do not contain promotional offers or sales incentives and are aimed at improving your product experience.

- **Marketing and Promotional Emails.** These emails are sent only with your explicit consent (Art. 6(1)(a) GDPR).

  They include:

  1) Newsletters;
  2) Product promotions or special offers;
  3) Invitations to webinars or events;
  4) Any other content intended to promote or advertise our products or services

We will only send you these types of emails if you have actively opted-in. You can withdraw your consent at any time by clicking the "unsubscribe" link in the footer of the email or by contacting us directly.

Consent Management and Record-Keeping. We maintain clear records of your preferences regarding communication. If you change your preferences or opt out of marketing, we will respect your choices immediately. Your communication preferences do not affect the delivery of essential transactional emails necessary to fulfil our obligations to you as part of the Services.

Avoiding Legal Ambiguity. To ensure compliance with applicable data protection regulations, including the GDPR:

(i) We do not mix marketing content with service-related messages;

(ii) All email templates undergo legal review before deployment;

(iii) We avoid misleading subject lines or content that may blur the line between marketing and functional communication.

Updating Your Preferences. You may update your communication preferences at any time by:

(i) Logging into your account and accessing the notifications section;
(ii) Contacting our support team at: support@kadam.net.

CHANGES TO THIS PRIVACY POLICY

We reserve the right to amend this Privacy Policy from time to time to reflect changes in the law, our data collection and data use practices, the features of our Platforms, or advances in technology.

Please check this page periodically for changes and refer to the “last updated” date at the top of the page to know if it has been revised since your last visit. If we make any changes to this Privacy Policy that we consider to be material to your consent, we will notify you of them.