

This is a translation provided for convenience only. The legally binding version of this document is the Russian-language original published at <https://wraxa.ai>. In the event of any discrepancy between this translation and the Russian-language version, the Russian-language version shall prevail.

# PRIVACY POLICY

of the Wraxa platform: Sites and Visuals

**Edition dated 24 October 2026**

## 1. Operator and Scope

1.1. Limited Liability Partnership «WRAXA», BIN 250940012660 (hereinafter, the "Operator"), collects and processes personal data in the course of operating the Wraxa platform. Address: Republic of Kazakhstan, city of Almaty, Bostandyk district, Nur Alatau microdistrict, Balzhan Boltirikov street, building 9, postal code 050045. Contact for data matters: [support@wraxa.ai](mailto:support@wraxa.ai).

1.2. The Policy applies to <https://wraxa.ai>, <https://visuals.wraxa.ai>, related official subdomains, the personal account, the official applications, the Wraxa Sites and Wraxa Visuals products, support requests, and data obtained in connection with their use (hereinafter, the "Platform").

1.3. Sites provides the creation, editing and publication of websites. Visuals provides AI tools for images, photographs, product cards, texts, content plans, video, animation, voice and other materials within the scope of the implemented features. The account and the token balance are shared; subscriptions to the products are separate.

1.4. The Policy takes into account the Law of the Republic of Kazakhstan "On Personal Data and Their Protection" and other applicable legislation. Personal data relate to an identified or identifiable individual and contain the corresponding identifiers. Data of an organization may be processed together with the data of its representatives, employees and customers.

1.5. The Policy describes the processing and does not replace consent required by law. A visit to the website in itself does not constitute unconditional consent to any purposes, advertising or publication of private content. Processing relies on consent obtained in a verifiable manner or on another basis provided for by law.

1.6. Third-party websites, banks, app stores, social networks and other services apply their own rules. Data of visitors to user websites are considered taking into account section 8; the Policy does not replace the documents of the owner of such a website.

## 2. What Data May Be Processed

2.1. Registration and account: identifier, email, phone number, the name and profile provided, language, country, sign-in method, verification statuses, dates of registration and sign-ins. When signing in via Google or Apple, information from the provider that the user has permitted is received. Passwords and sessions are processed by means of the authentication system; there is no need to disclose the password to support staff.

2.2. Purchases, subscriptions and settlements: product, one-time or recurring offer, plan, its price and included token quota, access term, consent to auto-renewal, subscription statuses, date, amount and currency of payment, order number, transaction and payment method identifiers, limited card information from the provider, refund requests, token credits and debits. Current prices and quotas are determined by the Offer and the terms of the specific purchase. The full card details and the security code are entered in the provider's payment form and are not requested by support.

2.3. Sites: description of the task and the business, AI prompts and correspondence with the assistant, page texts and structure, code and settings, images and files, domain, history of changes, publications and deletions, inquiries and other visitor data, if the user enables their collection by available means.

2.4. Visuals: prompts, scripts, product and business descriptions, photos, images, video, audio, references and the faces and voices in them, character and shoot settings, generation results and versions, content plans, information about tasks, downloads and publications. Materials may contain data of the user and of other people.

2.5. Photos, video and voice may make it possible to identify a person and require appropriate protection. If features for establishing identity are extracted in a particular processing operation, the requirements of law for biometric data apply. Uploading an image for generation does not grant unlimited permission to identify people or to use their likeness.

2.6. Integrations: account links and identifiers, permissions and technical connection keys, information and statistics permitted by the service. For the analysis of public sources, available posts, images, metrics and public profile data may be processed. The scope depends on the selected feature and the authority granted.

2.7. Technical data: IP address, approximate country based on IP, time of request, page and referral source, browser, device, operating system, application version, session identifiers, cookies and local storage, language and settings, usage events, errors, information on performance and security, and technical logs.

2.8. Communications: contact details, the content of emails and chats, attachments, requests concerning rights to materials, payments and violations, response history. When a separate application form is filled in, the information provided in it about the company, budget, timelines and contacts is processed.

2.9. For ordinary use, the Operator does not require a passport, an individual identification number (IIN), medical information, banking passwords or secrets protected by law. Excessive sensitive information or data that one has no right to process should not be uploaded. For a disputed request, proportionate information confirming identity, payment or authority may be required.

### **3. Sources, Purposes and Legal Bases**

3.1. Data are received from the user, the user's representatives, connected services and payment providers, from technical interaction, from lawfully accessible public sources and from requests of third parties. The availability of information on the internet does not cancel the requirements for its lawful use.

3.2. For the account and security, registration and technical data are processed: sign-in, contact verification, access recovery, abuse detection, and selection of the registration method available for the country and of the interface language.

3.3. To perform tasks, materials, prompts, results and technical information are used: website creation, editing, file storage, publication on the user's instructions, execution of AI generations, display of history, calculation of quotas and provision of the features of the paid product.

3.4. For settlements and the agreement, orders, subscriptions, consents, payments and tokens are used: activation of one-time access to Visuals and of subscriptions, separate renewal of Sites and Visuals, accounting for paid quotas, cancellation, refunds, reconciliation and mandatory accounting. The token spending history is also used to verify the conditions for a voluntary refund established by the Offer.

3.5. For support and the investigation of failures, requests, diagnostic logs, device data and necessary fragments of the affected materials are used. Employees and contractors are granted access to the extent necessary for the task. For usage analysis and advertising, the information described in sections 6 and 7 is used on a proper legal basis.

3.6. The legal bases include the consent of the data subject or their legal representative, and specific cases of processing without consent expressly permitted by law, for example a mandatory demand of an authorized body. The agreement in itself does not override separate consent where it is required for particular data, a particular purpose or a particular transfer.

3.7. Consent given through the interface relates to the purposes, categories of data, operations and recipients shown, in accordance with the Policy and the specific form. The Operator is entitled to record the version of the text, the date, the time and the confirmation of the choice. Publication and cross-border transfer require a proper legal basis, taking into account sections 4, 5 and 8. A new independent purpose requires a separate assessment of the legal basis.

## **4. Materials and External AI Services**

4.1. To fulfill a request, materials, the task text, parameters and necessary intermediate results may be transferred to external AI providers and technical intermediaries of the relevant feature. Depending on the operation, solutions of Google/Gemini, Anthropic, OpenAI, AtlasCloud, MiniMax, ElevenLabs and other connected providers are used, in compliance with the requirements of law.

4.2. In image transformation, synthetic photo shoots, animation and voice-over, facial photos, voice recordings, product images and references may be transferred. For speech recognition, audio is transferred. Such operations should be launched only where the rights and the necessary consent of the affected persons to the relevant actions, including a synthetic likeness and transfer to contractors, are in place.

4.3. Before sending other people's materials, the user checks the scope of the permissions and, where possible, removes unnecessary identifiers, metadata, contact details and private information. Detailed obligations are set out in the Offer. The mere fact of upload does not confirm that the user has lawfully obtained the rights to a third party's data.

4.4. Fulfilling a request may require storage and technical processing by the provider, security checks and service logs within the limits of the contract and the law. The Operator does not promise a complete absence of storage by all providers. Information about the recipient and the terms of a specific feature may be requested at [support@wraxa.ai](mailto:support@wraxa.ai).

4.5. The Policy does not give the Operator unconditional permission to use private individuals in advertising, to sell uploaded photos or to independently train its own general-purpose models on private content. A new purpose requires a proper legal basis and, where necessary, separate consent. This does not preclude lawful processing by an external provider to fulfill a request.

4.6. Private materials become publicly available upon the publication of a website, the posting of a publication, the granting of access via a link or another instruction of the user, to the extent specified by the user. Settings and consents are checked before taking the action. Deleting the source file does not guarantee the deletion of previously published copies held by independent third parties.

## **5. Recipients and Cross-Border Transfer**

5.1. Contractors may be engaged for authentication, database and file storage, hosting and content delivery, AI, acquiring, notifications, support, diagnostics and analytics. The current architecture uses, among others, Supabase, Vercel, TipTopPay, PostHog and Sentry; AI providers are listed in section 4. App stores and sign-in providers are involved when the corresponding purchase or sign-in method is chosen.

5.2. For public social media pages, specialized contractors may be used, including Apify. In the course of support and notifications, necessary information may be processed by communication services, including Telegram and connected messaging tools. The recipients actually involved depend on the features selected. Advertising recipients are described in section 7.

5.3. Recipients are provided with the data necessary for the purpose, with access segregation and applicable protection measures. Some recipients independently determine the processing within their payment, account and other services and apply their own legal bases. Engaging a contractor does not cancel the Operator's obligations.

5.4. When external infrastructure is used, certain operations may take place outside Kazakhstan, in the countries where the providers' services are hosted. Transfer is permitted only in compliance with the requirements of law, including the necessary consent or another basis and the requirements for protection in the recipient's country. The countries and recipients for a specific operation may be clarified with the Operator.

5.5. Mandatory requirements to store personal data within the territory of Kazakhstan remain in force regardless of foreign cloud and AI services. The Policy and consent to cross-border transfer do not cancel localization. The Operator is obliged to ensure a lawful procedure for storage and transfer; the existence of the Policy does not in itself confirm the location of each server.

5.6. Data may be provided to public authorities, courts and other persons upon a lawful mandatory demand, and to protect rights and investigate violations, to the extent permitted by law. In the event of a business transfer or reorganization, the necessary safeguards, notices and consents are maintained; the data do not become publicly available solely as a result of such a transfer.

## **6. Cookies, Analytics and Diagnostics**

6.1. Cookies and local storage are used for sign-in, security, language, interface settings, consent status and the operation of features. The browser allows such data to be restricted and deleted; disabling necessary mechanisms may affect sign-in and the operation of the Platform.

6.2. PostHog analyzes visits and events, the path to registration and payment, feature usage and errors. For an authorized user, events may be linked to the account identifier, email, referral source and subscription parameters. The project configuration uses the European PostHog address.

6.3. PostHog may capture recordings of interactions with the interface, actions, displayed content, the console and information about network requests. The settings provide for masking of values entered in input fields and do not include recording of network request bodies. This does not mean that all content displayed on the page is hidden: diagnostics and recordings may contain fragments of user materials.

6.4. Sentry monitors errors and performance and may receive device and network data, the user's identifier, email and name, the sequence of actions before an error and a session recording upon an error. The scope depends on the event. The information is used for diagnostics and to protect the operation of the Platform.

6.5. For optional analytics and session recording, an independent legal basis is assessed; consent to Meta does not automatically constitute consent to all tools. Where prior consent is required, the tools must be enabled only after it has been obtained. A request to opt out of optional processing may be sent to [support@wraxa.ai](mailto:support@wraxa.ai); processing necessary for security, settlements and compliance with the law is considered separately.

## **7. Advertising and Notifications**

7.1. Meta Pixel and server-side Meta Conversions API events (Meta Platforms Ireland Ltd. / Meta Platforms, Inc.) are used to measure and optimize advertising. Visits and permitted events, the page address, Meta cookies (`_fbp`, `_fbc`), the referral source, the IP address and browser data are processed. Upon the first confirmed payment for access, a Subscribe event may be transmitted with the time, amount, currency and order identifier in order to prevent double counting.

7.2. In the current implementation of the server-side Subscribe event, email, phone number, the content of AI tasks and card details are not included in the event. This description of a specific event does not mean that contact data are absent from other registration, support and settlement services.

7.3. For the EU/EEA, the United Kingdom, Switzerland and where the country cannot be determined, Meta is enabled after consent is given in the banner. In other regions, the procedure permitted by law applies, taking into account the user's choice. An explicit refusal takes precedence. The choice is stored together with the date and the version of the notice. It can be changed via "Cookie settings".

7.4. A refusal stops the subsequent transmission governed by that choice and does not automatically cancel lawful processing already carried out by the recipient. A request to delete or correct transmitted information may be sent to the Operator; Meta's procedures also apply.

7.5. For certain campaigns, Google Ads attribution and conversion tools are used, including click identifiers and registration or other target action events. Applicable consent and opt-out requirements are complied with; Meta settings do not constitute universal control over all advertising services.

7.6. Service messages concern sign-in, security, payments, access term, tasks and changes to the terms. Marketing mailings are sent on a proper legal basis; one may unsubscribe using the method indicated in the message or through support. Opting out of marketing does not stop necessary contractual correspondence.

## **8. Third-Party Data and Website Visitors**

8.1. The user shall have a lawful basis for transferring other people's data, using them in AI and publishing them. The required consent must cover the relevant purposes and recipients. For images, voices and data of minors, the authority of the legal representative is taken into account. The Platform is intended for adult users.

8.2. The owner of a website in Sites determines the purposes and composition of the inquiries, orders and visitor data the owner collects. The owner ensures notices, consents, cookie rules, retention periods and the handling of customer requests. The Operator performs technical processing to the extent of the available feature and the owner's lawful instruction, while retaining its own obligations under law.

8.3. The user is not entitled to promise their customers that no transfer to technical contractors will take place if such transfer is necessary for a connected feature. For an external form, chat, payments or analytics on their website, the user checks the provider's rules and the legal bases for processing.

8.4. A person who finds their data in someone else's project or Visuals result may write to [support@wraxa.ai](mailto:support@wraxa.ai) with a link to or the identifier of the material and a description of the violation. The Operator reviews the request, requests minimal confirmation where necessary, and takes lawful measures, including restricting access and engaging with the owner of the material.

## **9. Retention, Security and Deletion**

9.1. Data are stored no longer than necessary for the stated purpose, the agreement and the mandatory periods established by law. Materials and settings are stored for as long as access to the project and its history is needed; payments, consents, disputes and security records, within the limits of mandatory accounting and the protection of legal claims. The retention period for a category may be clarified with the Operator. Indefinite storage for an undefined purpose is not permitted by the Policy.

9.2. The end of a subscription is not equivalent to deletion of the account. Deleting an object affects data and links to the extent of the feature: for example, deleting a content plan does not always delete previously created standalone posts and videos. Stopping the processing of all data that can be deleted requires a separate request concerning the account.

9.3. A deletion request is sent to [support@wraxa.ai](mailto:support@wraxa.ai) with confirmation of account ownership. The Operator determines the information subject to deletion and the data that must be retained under law or in connection with outstanding obligations, and provides a response. At the same time, it is verified that auto-renewal of each product and app store purchases have been stopped.

9.4. Backups and logs are deleted within the applicable retention cycle, with further use restricted and mandatory periods observed. Independent copies held by recipients and records that a third party is obliged to keep are considered on the relevant basis. Instant destruction of all copies across the entire internet is not guaranteed.

9.5. The Operator takes proportionate legal, organizational and technical measures: access restriction, authentication, secure transmission over supported connections, role-based permissions, logging of requests and oversight of contractors to the applicable extent. Absolute security is not guaranteed; this does not cancel mandatory measures or liability for the Operator's own breaches.

9.6. The user protects sign-in credentials and the device, does not publish passwords and keys, and reports suspicious access. If a security breach is detected, the Operator limits its consequences and fulfills the obligations to notify authorities and affected persons if and within the time limits required by law.

## **10. Data Subject Rights and Requests**

10.1. Within the limits of applicable law, the data subject is entitled to learn about the existence of data, the purposes, sources, composition, recipients and periods of processing; to obtain access; to demand correction, supplementation, blocking or destruction in the established cases; to withdraw consent; and to appeal against unlawful processing.

10.2. To submit a request, write to [support@wraxa.ai](mailto:support@wraxa.ai) with the subject line "Personal data", describe the demand and provide information to locate the account or material. The Operator may request proportionate confirmation of identity or authority to protect against disclosure to unauthorized persons. Full payment details and the password are not required.

10.3. Requests are fulfilled within the time limits established by law. In particular, upon a permissible withdrawal of consent, processing is stopped or a reasoned refusal is provided within 15 working days, unless a different period is established by the applicable rule. Shorter mandatory periods may apply to certain demands for change, blocking or destruction.

10.4. Withdrawal does not render prior lawful processing unlawful. Retention may continue only where a basis remains, for example mandatory accounting or an outstanding obligation provided for by law; the basis is explained in the response. If a selected feature cannot be performed without the data, access to it may cease.

10.5. Additional mandatory safeguards of another applicable jurisdiction, including restriction of processing, objection or portability, are observed to the applicable extent. The choice of the law of Kazakhstan does not deprive anyone of inalienable rights. Contacting the Operator does not limit the right to lodge a complaint with an authorized body or a court.

## **11. Changes to the Policy**

11.1. The dated edition is posted at <https://wraxa.ai/documents/privacy-policy.pdf>. The Operator gives notice of any material change in purposes, recipients or processing by an available means; any necessary new consent is obtained before the processing. Publication of an edition does not constitute retroactive permission for another purpose.

11.2. The Policy is effective from its publication until it is replaced by a new edition. Access, payment and refunds are governed separately by the Offer: <https://wraxa.ai/documents/oferta.pdf>. Questions concerning privacy, access, correction, deletion and withdrawal of consent should be sent to [support@wraxa.ai](mailto:support@wraxa.ai).