

For EU

- [Terms of service](#)
- [Privacy policy](#)
- [Acceptable usage policy](#)
- [Cookie policy](#)

Terms of service

Last Updated: September 8, 2026

Welcome to our Service. These Terms of Service ("Terms") constitute a legally binding agreement made between you, whether personally or on behalf of an entity ("you," "user," or "consumer"), and IQBID Helios Limited, a company registered under the laws of the Republic of Seychelles with registration number 252002 and registered office at ____ ("Company," "we," "us," or "our").

These Terms govern your access to and use of our artificial intelligence (AI) model aggregation platform, website, and related applications (collectively, the "Service").

Please read these Terms carefully before accessing the Service. If you reside within the European Union (EU) or the European Economic Area (EEA), specific mandatory consumer protection laws and regulations apply to your usage, including the EU Artificial Intelligence Act (Regulation (EU) 2024/1689) and the EU Digital Services Act.

1. Eligibility and age restrictions

By registering an account or using the Service, you represent and warrant that you are at least eighteen (18) years of age. The Service is strictly intended for individuals who have reached the age of majority. If you are under 18, you are prohibited from creating an account or submitting any personal data or files to the Service.

2. Nature of the service & eu ai act compliance

The Company operates an online software aggregation interface that routes user queries to third-party artificial intelligence infrastructure networks (such as OpenAI, LLC and Google LLC) via secure Application Programming Interfaces (APIs).

EU AI ACT TRANSPARENCY DISCLOSURE: In strict compliance with Article 50 of the EU Artificial Intelligence Act (Regulation (EU) 2024/1689), the Company explicitly informs you that all text, images, documents, or outputs generated through this Service are created automatically by artificial intelligence algorithms and systems. The Service does not generate human-authored editorial content. By interacting with the Service, you acknowledge your awareness that you are interacting with an artificial intelligence system.

3. Subscriptions, fees, and payments

3.1. Subscription Tiers

Access to advanced AI models requires a paid tier ("Subscription Plan"). The fees, computational parameters, and prompt quotas applicable to each Subscription Plan are explicitly displayed on our checkout interface. All payments from EU users are securely processed by our third-party infrastructure payment processors.

3.2. **ONE-TIME TRANSACTIONS.**

All Credit Plans are provided via single, non-recurring transactions. Performance of the digital content begins immediately upon successful payment verification. In accordance with Article 16(m) of the EU Consumer Rights Directive, you explicitly agree to immediate performance and acknowledge that you lose your 14-day right of withdrawal once the digital content is delivered. No automatic renewals or latent billings are applicable to the Service."

3.3. Mandatory waiver of the eu right of withdrawal

UNDER DIRECTIVE 2011/83/EU ON CONSUMER RIGHTS, EU CONSUMERS GENERALLY POSSESS A STATUTORY RIGHT TO WITHDRAW FROM ONLINE CONTRACTS WITHIN FOURTEEN (14) CALENDAR DAYS WITHOUT GIVING ANY REASON.

HOWEVER, PURSUANT TO ARTICLE 16(M) OF SAID DIRECTIVE, THE RIGHT OF WITHDRAWAL DOES NOT APPLY TO THE SUPPLY OF DIGITAL CONTENT WHICH IS NOT SUPPLIED ON A TANGIBLE MEDIUM IF THE PERFORMANCE HAS BEGUN.

BY PURCHASING A SUBSCRIPTION PLAN AND CLICKING THE "SUBSCRIBE" OR "PAY" BUTTON, YOU EXPLICITLY REQUEST, AGREE, AND CONSENT TO THE IMMEDIATE PROVISION AND EXECUTION OF THE DIGITAL SERVICE. YOU ACKNOWLEDGE AND EXPRESSLY AGREE THAT ONCE ACCESS TO THE AI AGGREGATION INTERFACE, PROMPT LIMITS, OR TOKEN CAPACITY IS DELIVERED TO YOUR USER ACCOUNT, YOU COMPLETELY LOSE YOUR STATUTORY 14-DAY RIGHT OF WITHDRAWAL (RIGHT TO A REFUND).

4. Intellectual property and user materials

4.1. User Content

You retain all ownership, copyright, and intellectual property rights in the text prompts, questions, and files (images, audio, documents) that you upload or input into the Service ("User Content"). You represent that you possess all necessary legal rights and permissions to submit such User Content.

4.2. Licensing for Processing

To deliver the Service, you grant the Company a worldwide, non-exclusive, royalty-free, transactional license to host, cache, transmit, and route your User Content to third-party AI models (OpenAI, Google, etc.) strictly for execution.

4.3. AI Generated Outputs

The Company does not claim any copyright or ownership over the textual, visual, or structural materials generated by the aggregated AI models in response to your prompts ("Outputs"). The allocation of intellectual property rights over AI-generated outputs is subject to the national laws of your specific EU member state.

5. Disclaimer of warranties & limitation of liability

5.1. AI Accuracy and Hallucinations

You acknowledge that automated machine learning systems may occasionally generate inaccurate, incomplete, biased, or incorrect Outputs (commonly referred to as "AI hallucinations"). The Company acts strictly as an aggregation conduit and does not verify or guarantee the objective truthfulness, safety, or real-world utility of any generated Output.

5.2. Statutory Warranty Rights

Nothing in these Terms shall limit or exclude your statutory warranty rights as an EU consumer regarding digital services that fail to comply with subjective or objective conformity requirements.

5.3. Limitation of Liability

To the maximum extent permitted by the mandatory consumer protection laws of your country of residence, the Company's total liability for any damages arising out of or in connection with the Service shall be limited to the total amount paid by you to the Company during the twelve (12) months preceding the event giving rise to liability. The Company shall not be liable for any indirect, unpredictable, or consequential losses, or losses resulting from your breach of our Acceptable Usage Policy.

6. Mandatory eu dispute resolution & jurisdiction

6.1. ODR Platform

The European Commission provides an online dispute resolution platform, which you can access at <https://europa.eu>. We prefer to resolve any disputes directly with you via email at legal@iqbid.ai.

6.2. Governing Law

These Terms and your use of the Service shall be governed by the laws of the Republic of Seychelles. However, as an EU consumer, you enjoy the protection of the mandatory statutory provisions of the law of the EU Member State where you have your habitual residence.

6.3. Forum and Venue

Any legal action or dispute arising out of these Terms shall be brought before the competent courts of the Republic of Seychelles, OR, at your sole election, before the competent national courts of your EU country of residence.

7. Contact information

For any formal inquiries regarding these EU Terms, please contact our corporate department at:

- **Email:** legal@iqbid.ai
- **Corporate Entity:** IQBID Helios Limited
- **Registered Address:**

Privacy policy

Last Updated: September 8, 2026

IQBID Helios Limited ("Company," "we," "us," or "our"), a company registered under the laws of the Republic of Seychelles, operates as the Data Controller under Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation — "GDPR").

This Privacy Policy applies exclusively to data subjects residing within the European Union (EU), the European Economic Area (EEA), and Switzerland ("EU Users") who access our artificial intelligence (AI) model aggregation platform, website, and associated infrastructure (the "Service").

1. Legal bases for processing personal data

In strict accordance with Article 6 of the GDPR, we process your personal data only when we have a valid legal basis:

- **Performance of a Contract (Art. 6(1)(b) GDPR):** To activate your account, provide access to our Artificial intelligence computing aggregation interface, allocate query quotas, and securely manage your permanent subscription plan using a Payment Service.
 - **Legitimate Interests (Art. 6(1)(f) GDPR):** To detect, prevent, and mitigate infrastructure fraud, enforce our Acceptable Usage Policy, and maintain the absolute security of our technical network.
 - **Explicit Consent (Art. 6(1)(a) GDPR):** To utilize your submitted text prompts, questions, or uploaded digital files for the ongoing software optimization, fine-tuning, and internal algorithmic machine learning training of our internal systems.
-

2. Categories of personal data we collect

We collect and process the following categories of data regarding EU Users:

- **Account Identifiers:** First name, last name, corporate or personal email address, automated online identifier, and encrypted password credentials.
- **Technical Log Data:** IP address, device fingerprints, operating system type, browser parameters, timestamps of individual requests, and interface interaction metrics.
- **Financial Transactional Data:** The logs of billing history, currency conversion, transaction statuses, and payment identification numbers are synchronized with the Payment Service. We strictly do not hold or store raw payment card credentials.

- **User Inputs and Files:** The quantitative content of text queries and any integrated digital files (images, PDF documents, text sheets, audio material) that you actively upload to the interface ("User Content").
 - **AI-Generated Outputs:** Synthetic text, media, or data structures generated automatically by third-party downstream AI architectures in fulfillment of your prompt demands.
-

3. Recipients of personal data and sub-processors

To perform an AI model aggregation function, we securely transfer anonymized or raw user text queries and digital files via secure API channels to third-party artificial intelligence infrastructure developers acting as our independent infrastructure suppliers (Sub-processors), including but not limited to:

- **OpenAI, LLC** (United States)
- **Google LLC** (United States)
- **Anthropic, PBC** (United States)

Whenever personal data is transferred outside the EEA to countries not recognized as providing an adequate level of data protection, we ensure that appropriate safeguards, such as Standard Contractual Clauses (SCCs) adopted by the European Commission, are integrated into our supplier API enterprise contracts.

4. Strict protocol for ai model training and machine learning

The Company fine-tunes its proprietary software routing logic and underlying open-source machine learning matrices using interaction data.

MANDATORY EU CONSENT FRAMEWORK: THE COMPANY EXPLICITLY RECOGNIZES THAT YOUR SUBMITTED USER CONTENT AND UPLOADED FILES MAY CONTAIN SENSITIVE PERSONAL RECOLLECTIONS OR IDENTIFIERS. THE COMPANY WILL NEVER UTILIZE USER INPUTS OR FILES COLLECTED FROM EU USERS FOR MACHINE LEARNING INDUCTION OR AI MODEL TRAINING PURPOSES UNLESS YOU HAVE ACTIVELY GIVEN YOUR EXPLICIT, UNFORCED, INFORMED PRE-TRANSACTION CONSENT (OPT-IN) DURING YOUR SERVICE ONBOARDING REGISTRATION.

If you have granted consent, you retain the absolute statutory right to revoke your consent at any time without negative consequences or billing alterations by toggling the data-use controller in your Account Settings panel or by emailing privacy@iqbid.ai.

5. Data storage and localization

We store and process all infrastructure data, user profiles, and session caches of EU Users on secure cloud servers physically located within the territory of the European Union (EU/EEA).

6. Your mandatory gdpr privacy rights

As an EU/EEA data subject, you possess extensive statutory protections under Chapter III of the GDPR:

- **Right of Access (Art. 15 GDPR):** The right to request copies of your personal data held by us, alongside a comprehensive breakdown of our current automated processing paths.
- **Right to Rectification (Art. 16 GDPR):** The right to compel the correction of inaccurate or incomplete personal data records.
- **Right to Erasure / "Right to be Forgotten" (Art. 17 GDPR):** The right to request the complete, permanent scrubbing of your profile logs, historical chat contexts, and uploaded data assets, subject to regulatory transaction record retention mandates.
- **Right to Restriction of Processing (Art. 18 GDPR):** The right to restrict data processing under specific civil dispute conditions.
- **Right to Data Portability (Art. 20 GDPR):** The right to demand that your stored historical materials are exported to you in a structured, machine-readable, commonly used software format.
- **Right to Object (Art. 21 GDPR):** The right to immediately halt any processing activities predicated on our corporate Legitimate Interests.

To assert any of your statutory GDPR rights, please submit a verified communication to our global privacy enforcement officer at privacy@iqbid.ai from your registered email profile.

7. Data storage and cache retention term

We store account profile IDs and billing information for as long as your user account remains active, or to fulfill the financial accounting requirements provided by the Payment System.

To manage operational cloud engineering overhead, User Content (prompts and uploaded documents) along with generated Outputs are cached in an encrypted state on our servers to enable your active workspace view. Cached session assets are automatically and permanently deleted from our records ninety (90) calendar days from generation, unless you manually delete your chat log panel earlier.

8. Right to lodge a complaint with a supervisory authority

If you believe that our aggregation platform processes your files or personal data in a manner that infringes the mandates of the GDPR, you possess the absolute right to lodge a formal statutory

complaint with a competent data protection supervisory authority within the EU Member State of your habitual residence, place of work, or place of the alleged infringement.

9. GDPR compliance contact

- **Email Communication:** privacy@iqbid.ai
- **Attn:** Data Protection Officer (DPO)
- **Corporate Controller Entity:**

Acceptable usage policy

Last Updated: September 8, 2026

This Acceptable Usage Policy ("AUP") defines the strictly prohibited boundaries, behavioral limits, and content restrictions governing your operational interaction with the artificial intelligence (AI) model aggregation platform, system, and infrastructure (collectively, the "Service") provisioned by IQBID Helios Limited ("Company," "we," "us," or "our").

This AUP is integrated directly into, and forms an inseparable part of, our European Union Terms of Service. It applies directly to all users accessing the Service from the European Union (EU) or European Economic Area (EEA) ("EU Users"). Because our system routes transactional inputs via API to third-party infrastructure entities (including OpenAI, LLC and Google LLC), you are statutory-mandated to strictly respect both our corporate standards and the downstream application rules enforced by those underlying ~~III~~ networks.

1. Absolute prohibitions under the eu ai act and dsa

In strict compliance with the EU Artificial Intelligence Act (Regulation (EU) 2024/1689) and the Digital Services Act (Regulation (EU) 2022/2065), you are explicitly prohibited from submitting text queries, semantic instructions, prompts, or uploading any digital files (documents, images, media) (collectively, "User Inputs") designed to execute or generate the following:

A. Subliminal Manipulation and Behavioral Distortion

- **Cognitive Manipulation:** Actively prompting or forcing AI models to generate text, audio scripts, or psychological frameworks that deploy subliminal techniques beyond a person's consciousness to materially distort a person's behavior in a manner that causes or is likely to cause physical or psychological harm.
- **Exploitation of Vulnerabilities:** Generating targeted outputs designed to exploit any specific vulnerabilities of a specific group of persons due to their age, physical, or mental disability, to distort their baseline real-world actions.

B. Prohibited Biometric Systems and Social Scoring

- **Biometric Categorization:** Uploading photographic directories or facial data to classify natural persons individually based on protected characteristics (e.g., race, political opinions, trade union membership, religious beliefs, sexual orientation).
- **Untrustworthy Social Scoring:** Requesting models to evaluate, score, or categorize natural persons over a certain period based on their social behavior or known personality characteristics, leading to detrimental or unfavorable treatment in real-world

environments.

C. Illegal European Content, Violence, and Child Safety

- **Illegal Content under the DSA:** Submitting or requesting any material that constitutes illegal hate speech, xenophobic manifestos, terrorist propaganda, or operational tutorials on fabricating illicit weapons, explosives, or chemical agents.
- **Child Sexual Abuse Material (CSAM):** The Company enforces an absolute zero-tolerance threshold regarding Child Sexual Abuse Material or Child Sexual Exploitation and Abuse (CSAE). Any structural detection of material depicting minors in an exploitative or sexually explicit context will result in a permanent infrastructure ban and mandatory reporting to European law enforcement bodies (Europol/national offices).

D. Systemic Deepfakes, Deception, and Copyright Infringement

- **Deceptive Media (Deepfakes):** Generating or mutating imagery, audio, or video files that appear authentic but are synthetic ("Deepfakes") without clearly, explicitly, and permanently tagging or embedding machine-readable watermarks indicating that the content has been artificially generated or manipulated, as mandated by the EU AI Act.
- **API Harvesting and Reverse Engineering:** Utilizing systemic scraping macros, extraction web-bots, or automated loaders to extract the synthetic algorithmic training weight arrays, specific prompt configurations, or operational boundaries of our internal routing layers.

2. Moderation conduits and compliance complaints

To satisfy our statutory infrastructure duties under the Digital Services Act:

- **Automated Content Classification:** User Inputs and AI-generated Outputs are dynamically scanned by automated safety classifiers to identify high-probability systemic policy breaches before transmission across external provider nodes.
- **Notice and Action Mechanism:** If you identify any content hosted on or generated through our Service that violates local EU Member State laws or this AUP, you possess a legal right to submit a formal notification to our security department at abuse@iqbid.ai.

3. Structural account termination and financial penalties

If the Company flags clear indicators that your account interaction routines violate the mandates of this AUP, or present an immediate threat of triggering API key revocations from our primary upstream suppliers (OpenAI, Google, etc.), we will execute decisive technical actions.

CONSEQUENCES OF MATERIAL BREACH:

1. **Instant Infrastructure Revocation:** Permanent de-activation of your authorization profile, workspace partitions, and stored cache history panels without prior notification.
2. **Cancellation of balances under the agreement:** All active subscription days for prepayment, quotas for tokens and credit units processed using the Payment Service **will be permanently canceled as an automatic compensation fee provided for in the agreement to compensate** for administrative costs for moderation.
3. **Regulatory Disclosure:** The Company will actively cooperate with competent European data protection authorities and national markets supervisors if a formal inquiry is executed regarding illegal generative workflows.

Cookie policy

Last Updated: September 9, 2026

[INSERT SEYCHELLES COMPANY NAME] ("Company," "we," "us," or "our"), a company registered under the laws of the Republic of Seychelles with registration number [Insert Number], issues this Cookie Policy for users residing within the European Union (EU), the European Economic Area (EEA), and Switzerland ("EU Users").

This Cookie Policy explains how we deploy cookies and similar tracking technologies (collectively, "Cookies") when you interact with our artificial intelligence (AI) model aggregation service, website, and associated infrastructure (the "Service"). This Policy is compliant with the General Data Protection Regulation (GDPR) and the EU ePrivacy Directive (Directive 2002/58/EC).

1. What are cookies and tracking technologies?

Cookies are small text files that are placed on your computer or mobile device by a website server when you access an online service. They are utilized to make websites work efficiently, provide analytics, and maintain user preferences.

- **First-Party Cookies:** Cookies set directly by us to maintain your account session.
- **Third-Party Cookies:** Cookies placed by independent infrastructure and analytical service providers integrated into our system.

2. Categories of cookies we deploy

In strict compliance with EU regulations, we classify the Cookies used on our Service into the following categories:

- **Strictly Necessary Cookies:** These Cookies are technically essential to enable you to navigate our website and access secure areas, such as your User Dashboard. They manage your active login session and facilitate transactional checkouts via our third-party Payment Processors. Under the ePrivacy Directive, **these Cookies do not require your prior consent** and cannot be disabled through our consent banner.
- **Analytical and Performance Cookies (Consent Required):** These Cookies allow us to recognize and count the number of visitors and see how users move around our interface. This data helps us monitor server loads, identify system errors, and optimize our network routing pathways.
- **Functional Cookies (Consent Required):** These Cookies are used to recognize you when you return to our Service. They enable us to personalize our content for you and remember your preferred configurations (such as your default selected AI model, computational limits, or interface dark/light mode preferences).

3. Data sharing protocol and interaction with ai models

Our Service operates as a technicalAggregation Conduit. When you submit a text prompt or upload a file into our interface, the raw text or binary payload is transmitted securely via backend API tokens to international AI infrastructure developers (including OpenAI, LLC and Google LLC).

Please note that standard frontend browser Cookies stored on your local device **are never** shared with, transmitted to, or read by third-party AI developers during these API transactions. Your browser Cookies strictly manage your localized session state with our hosting servers.

4. The mandatory eu consent framework (how to control cookies)

Under the GDPR and ePrivacy Directive, you have absolute statutory control over non-essential tracking technologies.

- **Cookie Consent Banner (Strict Opt-in):** When you access the Service for the first time from an EU IP address, a Cookie Consent Banner will block the deployment of all Analytical and Functional Cookies by default. These non-essential Cookies will only be executed if you provide explicit, affirmative, unforced consent by clicking "Accept All" or checking specific categories in our Cookie Settings panel.
- **Managing Preferences:** You can alter, update, or completely revoke your cookie consent selections at any time by clicking the interactive "Cookie Settings" link located permanently in the footer of our website.
- **Browser Controls:** You may also block or delete cookies by configuring your internet browser settings. However, please be advised that disabling Strictly Necessary Cookies will severely disrupt your ability to log in and utilize the AI aggregation platform.

5. Policy amendments

The Company reserves the right to modify this EU Cookie Policy to reflect technological shifts or updates in European data protection case law. Any structural modifications will become immediately active upon the posting of the revised text on this page.

6. Contact and data protection officer

For any inquiries regarding this Cookie Policy or our data tracking frameworks, please contact our designated compliance team at: privacy@iqdid.ai