

PRIVACY POLICY (GDPR COMPLIANCE)

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. 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.

6. 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.

7. 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.

8. GDPR COMPLIANCE OFFICER CONTACT

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

Версия #4

Hostmaster создал 2026-09-08 14:13:03 UTC

Hostmaster обновил 2026-09-08 14:23:04 UTC