

ComIO.Studio Privacy Policy

Effective date: March 24, 2026

1. Operator and Data Controller

The controller of personal data (within the meaning of the GDPR) processed in connection with ComIO.Studio is:

Sebastian Pietrasiak ul. Patriotów 3A 32-593 Żarki Poland Email: info@comio.studio

(hereinafter: “**Operator**”)

The Operator is the creator and publisher of the ComIO.Studio Application — a desktop application for serial communication with a built-in AI Assistant — and the controller of personal data within the meaning of the GDPR. Throughout this Privacy Policy, the term “Operator” also encompasses the role of data controller.

2. Scope and Principles of Processing

ComIO.Studio operates as a **desktop application installed on the User’s device**. Data entered into it, such as port configurations, logs, terminal data, macros, scripts, and locally stored AI chat history, is generally processed and stored **locally on the User’s device**. The Operator does not have access to it, except for data knowingly sent by the User to online services, such as license activation and validation, payments, voluntary features, and AI queries in Managed Mode, in accordance with this Privacy Policy.

2.1 What Data Does NOT Reach the Operator

- Serial port configurations and terminal sessions
- Data buffer contents (received/sent bytes)
- Logs saved to file
- User macros (M1-M6), triggers, Lua scripts
- Files opened/sent by the user
- AI chat history (stored locally, subject to AI query content sent by the User in Managed Mode pursuant to §3.2 and §4.1)

2.2 What the Operator Processes – General Principle

The Operator processes only data necessary for:

- installation and conversion analytics (all versions, including free) — Installation Data;
- fulfilling paid plans (subscription / one-time license) — Operational Data;
- processing AI queries in Managed Mode;
- voluntary features (feedback, surveys, diagnostics) — if the User consents.

The detailed scope of data is described in §3.

2.3 AI Assistant Operating Modes

The AI Assistant may operate in one of two modes, which differ in the scope of data processed by the Operator:

	Managed Mode	BYOK Mode
Query flow	Device → Operator's Server → AI Provider → response → User	Device → AI Provider (directly) → response → User
Operator sees query content	Yes (temporarily, for processing and diagnostics)	No
Operator bills tokens	Yes (credits)	No
API key	Operator's	User's (stored locally)

3. Scope of Processed Personal Data

3.0 Installation Data — All Versions (Including Free)

Upon first launch, the Application generates an **anonymous installation identifier** (UUID) and registers it on the Operator's server. This record is created regardless of whether the User uses the free or paid version.

Data Category	Source	Purpose
Installation identifier (UUID)	Generated locally at first launch	Installation identification, analytics, free → paid conversion tracking
Application version	Application	Analytics, compatibility, update planning
Operating system and version	Application	Analytics, compatibility, diagnostics
Date of first launch	Application	Analytics, user cohorts
Dates of subsequent launches	Application	Activity analytics, user retention
Plan type (free / paid)	Application	Conversion analytics
Conversion date free → paid	Application / payment provider	Conversion analytics
Interface language	Application	Analytics, localization planning

The installation identifier is not linked to personal data (email address, name) until the User upgrades to a paid plan. Upon conversion to a paid plan, the installation record is linked to Operational Data (§3.1).

Legal basis: Art. 6(1)(f) GDPR (legitimate interest of the Operator: product analytics, conversion measurement, development planning).

3.1 Common Data — All Paid Plans

The following data is processed regardless of the selected plan (credit subscription, BYOK subscription, one-time BYOK license):

Data Category	Source	Purpose
---------------	--------	---------

License key	Generated at purchase	License identification
Plan type and license type	Checkout / payment provider	License management, analytics
Email address	Payment provider / User	Customer support, license issues, service-related contact
Name / alias	Payment provider / User	Customer identification
Country	Payment provider	Analytics, legal requirements, billing
Transaction currency	Payment provider	Billing, analytics
Payment method	Payment provider	Analytics, diagnostics
License credential	Generated at activation	Verification of access to paid features (stored locally on the User's device; its validity or status may be validated by the Operator's server)

Legal basis: Art. 6(1)(b) GDPR (performance of a contract) and Art. 6(1)(f) GDPR (legitimate interest: customer support, diagnostics, analytics, abuse prevention).

3.2 Additional Data – Managed Mode

The following data is processed **exclusively** in credit subscriptions (Managed Mode):

Data Category	Source	Purpose
Credit balance and cycle dates	Billing system	AI service delivery
AI query metadata (timestamp, model, token usage, status)	Proxy server	Diagnostics, billing, monitoring
AI query content	Proxy server (temporarily)	Request processing, diagnostics, abuse prevention

AI query content is processed for the purpose of delivering the service. Only exceptionally may it be temporarily processed also to the extent necessary for security diagnostics, error resolution, or abuse prevention, in accordance with the data minimization principle. Diagnostic logs may

exceptionally contain limited fragments of AI query content and are deleted without undue delay once the purpose has been fulfilled.

Legal basis: Art. 6(1)(b) GDPR (performance of a contract — AI service delivery) and, to the extent necessary for diagnostics, service security, and abuse prevention, Art. 6(1)(f) GDPR (legitimate interest of the Operator).

3.3 Data in BYOK Mode

In BYOK Mode (BYOK subscription and one-time BYOK license), the Operator **does not process** query content or AI responses. Communication occurs directly between the User's device and the external AI provider.

In this mode, the Operator processes **Installation Data** (§3.0) and **Common Data** listed in §3.1.

The API key is stored locally on the User's device and is not transmitted to the Operator's infrastructure.

Note: The data processing practices of the AI provider selected by the User (e.g. OpenAI, Anthropic, OpenRouter) are governed by that provider's privacy policy and terms of service. The Operator encourages Users to review them before using BYOK Mode.

3.4 Voluntarily Provided Data

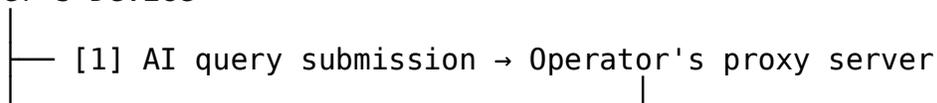
The Application may offer features allowing Users to voluntarily provide data (feedback, survey responses, diagnostic data, etc.). Participation is always voluntary and is not a condition for using the Application.

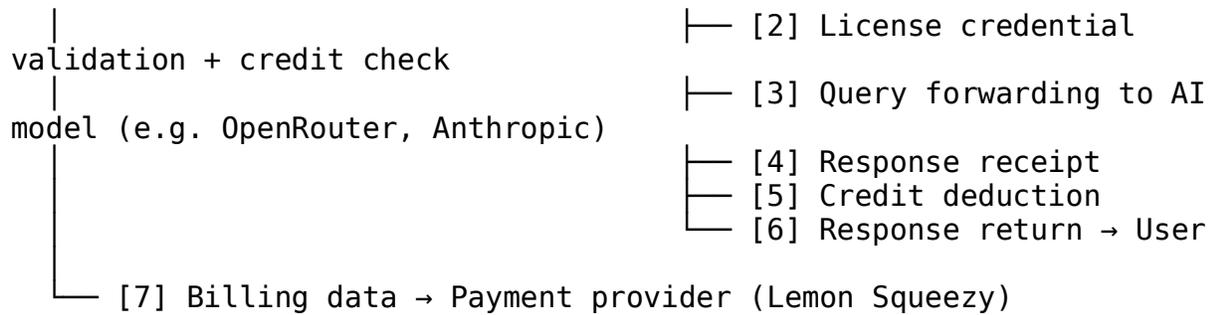
Legal basis: Art. 6(1)(a) GDPR (consent). The User may withdraw consent at any time, which does not affect the lawfulness of processing carried out prior to withdrawal.

4. Data Flow — Technical Details

4.1 Managed Mode

User's Device

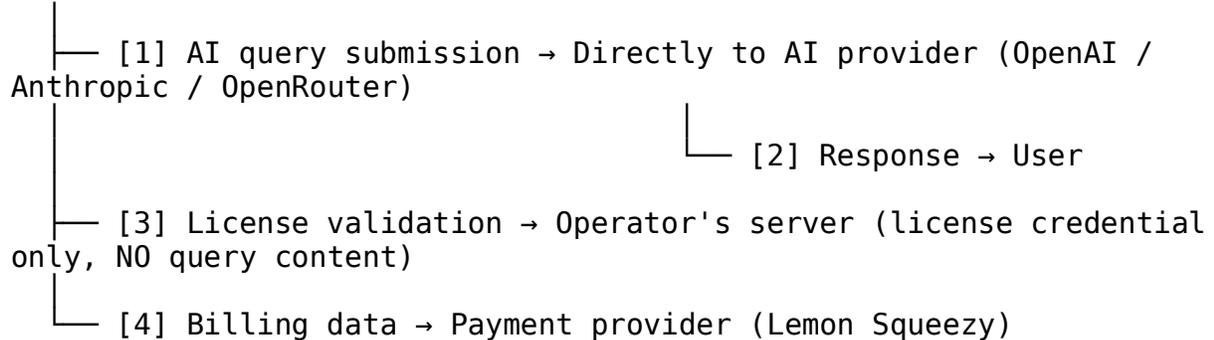




The Operator processes query content generally in transit and on a non-persistent basis — to the extent necessary to forward it to the AI model and return the response. Content is not permanently stored, subject to short-lived diagnostic logs created in accordance with data minimization principles and applicable retention periods.

4.2 BYOK Mode

User's Device



In BYOK Mode, the Operator **does not see** query content, AI responses, or token usage. The only communication with the Operator's server is license validation (license credential + plan type).

5. Data Retention Period

Category	Retention Period
Installation Data (\$3.0) — free version	Duration of installation activity + 1 year from last launch; then anonymized
Installation Data (\$3.0) — after	Same as Common Data (\$3.1)

conversion to paid plan Common Data (§3.1) — subscriptions	Subscription period + 90 days, unless longer retention is required by law, in particular tax or accounting regulations, or is necessary for the establishment, exercise, or defence of legal claims
Common Data (§3.1) — one-time license	Period necessary to maintain activation and license support + 90 days after permanent deactivation or termination of support
Additional Data — Managed Mode (§3.2), excluding AI query content AI query content (Managed Mode)	Subscription period + 90 days Transit only; temporary diagnostic logs deleted without undue delay once the purpose has been fulfilled
Voluntary data (§3.4)	Until consent withdrawal or until processing purpose is fulfilled

After the retention period:

- **Personal data** (email address, name) is **deleted or anonymized**.
 - **Analytical data** (country, currency, payment method) is **anonymized** within the same timeframe.
 - **Data anonymized** in a manner that prevents identification of a natural person may be retained longer, including indefinitely, for statistical, analytical, and billing purposes.
-

6. Data Recipients

Personal data may be shared with the following categories of recipients:

Recipient	Purpose	Data
Payment provider (Lemon Squeezy, Merchant of Record)	Payment processing	Transaction data
Cloudflare	Hosting, CDN and	Operational data and —

	application infrastructure	in Managed Mode — data technically necessary for processing AI queries
AI model provider (Managed Mode)	AI query processing	Query content (in transit)

The Operator does not sell personal data to third parties. Data is shared only to the extent necessary for service delivery.

In BYOK Mode, AI query content is transmitted directly by the User to the selected AI provider. Such provider operates in this regard outside the scope of data sharing carried out by the Operator, and the applicable data processing rules are determined by that provider’s privacy policy.

7. Data Transfers Outside the EEA

The Operator may configure infrastructure services so that data is stored in the EU/EEA; however, certain technical operations of the infrastructure provider may involve processing data outside that area, in accordance with that provider’s documentation and terms.

In Managed Mode, AI query content may be transferred to AI model providers processing data outside the EEA, including in the US, using appropriate mechanisms legalising the transfer in accordance with the GDPR, in particular:

- **Standard Contractual Clauses** (SCCs) within the meaning of Art. 46(2)(c) GDPR; or
- **Adequacy decision** — if the recipient is located in a country covered by such a decision; or
- other lawful transfer mechanisms, if permitted by applicable law.

In BYOK Mode, the transfer of query content to the AI provider occurs directly from the User’s device — the Operator does not participate in this data flow and does not control the processing location.

8. User Rights

Under the GDPR, you have the following rights:

Right	Description
Access (Art. 15)	Information about processed data and a copy thereof
Rectification (Art. 16)	Correction of inaccurate data

Erasure (Art. 17)	Deletion of personal data to the extent that there is no legal basis for continued processing arising from applicable law, the Operator’s legitimate interest, or the need to establish, exercise, or defend legal claims. Where appropriate, personal data will be deleted, and analytical or billing data may be anonymized
Restriction (Art. 18)	Restriction of processing in certain cases
Portability (Art. 20)	Receiving data in a machine-readable format
Objection (Art. 21)	Objection to processing based on legitimate interest
Withdrawal of consent (Art. 7(3))	For data processed based on consent (§3.4); withdrawal does not affect the lawfulness of prior processing

How to exercise your rights: Send a request to **info@comio.studio**. A response will be provided within the time required by applicable law.

9. US Users – California Privacy Rights (CCPA/CPRA)

If you use the Application as a **California resident**, you have the following rights under the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA):

Right	Description
Right to Know	You have the right to know what personal data we collect, for what purposes, and to whom it is disclosed
Right to Delete	You have the right to request

Right to Correct

deletion of your personal data, subject to exceptions permitted by law

You have the right to request correction of inaccurate personal data

Right to Opt-Out of Sale or Sharing

The Operator does **not sell** or **share** personal data as defined under CCPA/CPRA for cross-context behavioral advertising purposes

Right to Non-Discrimination

Exercising any of the above rights will not result in discriminatory treatment

To exercise these rights, contact us at **info@comio.studio**. We will verify your identity and respond within the time required by applicable law.

Users in other US states may have similar rights under applicable state privacy laws. We handle data requests regardless of state of residence.

10. Data Security

The Operator implements commercially reasonable technical and organizational measures designed to protect personal data from loss, misuse, unauthorised access, disclosure, alteration, or destruction. However, no method of transmission over the Internet or method of electronic storage is completely secure.

11. Cookies and Local Data

ComIO.Studio as a desktop application **does not use cookies**.

The comio.studio website may use only essential cookies or similar technologies required for its proper functioning (e.g. bot protection, rate limiting). Currently, the website does not use analytics, advertising, or tracking cookies.

Detailed information about cookies used on the website is provided in the separate [Cookie Policy](#).

12. Children's Data

ComIO.Studio is not intended for persons under **18 years of age**. The Operator does not knowingly collect personal data from persons below this age. If the Operator becomes aware of processing data of a person under 18, steps will be taken to promptly delete such data.

13. Changes to the Privacy Policy

The Operator reserves the right to update this Privacy Policy. Users will be notified of material changes with **reasonable advance notice** within the Application, on the website, or via email (if an address is available).

Continued use of the Application after the changes take effect means using the Application on the terms set out in the current version of the Privacy Policy, without prejudice to User rights under applicable law.

14. Contact and Complaints

For matters related to personal data:

- **Email:** info@comio.studio
- **Address:** Sebastian Pietrasiak, ul. Patriotów 3A, 32-593 Żarki, Poland

If you believe that the processing of your personal data violates applicable data protection laws, you have the right to lodge a complaint with the competent supervisory authority. In Poland, this is:

President of the Personal Data Protection Office (PUODO) ul. Stawki 2, 00-193 Warsaw <https://uodo.gov.pl>