Privacy Policy

Effective 22 Nov 2026 Version 2.0 For everyone

The short version

- What you send is passed to the AI provider serving the model you choose, which may keep or use it under its own terms.
- Your chats, files and memory in the web app are stored in your browser, not on our servers.
- We don't train our own models on your prompts or outputs, and we don't sell your personal information for money.
- We keep account, billing, usage and security records, including IP and device data, to run the service and handle payment disputes.
- Our API servers are in Germany and our main database is in the United States.

This summary helps you find your way. The full text below is what applies.

This Privacy Policy explains how the operator of Electron Hub ("**Electron Hub**", "**we**", "**us**") collects, uses, shares and protects personal data when you use electronhub.ai and its subdomains (including www, app, api, ws, docs, benchmark, forum, status, legacy, tos, privacy and legal), our API and related services (the "**Service**"). It uses the defined terms of our Terms of Service.

1. Who we are and how to contact us

The controller of your personal data is the operator of Electron Hub.

- Privacy questions and requests: support@electronhub.ai (subject "Privacy")

When you use the Service on behalf of an organisation that has its own agreement with us covering personal data, we may act as a processor for that organisation for some data; that agreement then governs.

2. Personal data we collect

2.1 Account and sign-in data. When you sign in with Google or Discord, we receive and store your account identifier, name or username, email address (only if the provider has verified it), and profile picture. We store whether your email, phone and Discord account are verified, your plan, balances, settings and notification preferences, and records of acceptance of our Terms.

2.2 Phone verification. If you verify a phone number, the code is sent by Google Firebase Authentication, we check the number's type (for example, whether it is a VoIP number) with Twilio Lookup, and we store the number and its verification status.

2.3 Profile pictures. If you upload an avatar, it is stored with a third-party file host at a URL anyone with the link can open. Default avatars are generated by DiceBear from your username.

2.4 Requests and content. When you use a Model, we receive the content of your request, such as prompts, messages, system instructions, files, images, audio, tool definitions and tool results ("**Input**"), and the Model's response ("**Output**"). We process it in transit to fulfil the request. We do **not** keep a general archive of your conversations, but some content is kept in the cases listed in Section 5, including error diagnostics that can contain a whole conversation up to the failed request.

2.5 Usage and billing records. For each request we record metadata such as the time, Model, route and provider, token counts, cost, status, the API key used (masked), your IP address and country. We keep daily usage totals per account, lifetime usage totals per Model, and records of credits, plans, purchases, refunds and disputes.

2.6 Payment data. Payments are processed by our payment providers (Section 4). We do not receive or store full card numbers. We receive order and payment details such as the amount, currency, product, order and subscription identifiers, payment status, the billing email and name used, country, and for some providers the card country, the IP address used at checkout and risk signals. For cryptocurrency payments we receive the transaction and amount details from our processor.

2.7 Sessions and security data. For each signed-in session we store a hashed session token, your browser's user agent, a device label, the IP addresses used when the session started and last refreshed, and the approximate location (country, and sometimes city) derived from the IP address. Our network provider, Cloudflare, passes us the approximate location of each request's IP address (country, region, city, postcode and coordinates), applies rate limits per IP address, and runs bot detection on our websites. We also use third-party IP-intelligence services to detect VPNs, proxies and data-centre traffic.

2.8 Device fingerprints and anti-abuse signals. To prevent multiple-account and rewards abuse, we collect device and browser characteristics (for example screen, graphics, audio and hardware properties, fonts, time zone and language) and compute a device identifier. The app computes it when it loads, and we link it to your account and IP address when you claim rewards. The Rewards page on our website collects more detailed signals (including canvas, graphics, audio, screen, processor and keyboard characteristics) to verify a claim. We also keep counts of free accounts created per IP address, records of IP addresses and networks used with Coding Plan keys, and hashes of deleted accounts' email addresses to prevent re-registration abuse.

2.9 Coding Plan (DevPass) data. To enforce fair use, for Coding Plan keys we keep recent request samples (short excerpts of up to 20 recent prompts and responses, and further samples for keys flagged for review), prompt fingerprints, the working-directory paths that coding tools send, request timing, and the IP addresses and networks used.

2.10 Support and communications. If you contact us by email or Discord, we keep your messages and the information you provide. We keep records of the service and notification emails we send you.

2.11 Data stored in your browser. The web app stores some data locally on your device, not on our servers: your chats, workspace files, agent memory and search indexes, skills, settings, your API key and session tokens (see Section 9).

2.12 Website analytics and advertising. Our websites use Google Analytics, Google AdSense and Cloudflare Web Analytics, which collect information about your visit, device and interactions using cookies or similar technologies (Section 9). Our community forum and status page are run by providers that use their own analytics, support and advertising tools. The Rewards feature sends you to third-party ad and link-shortener pages, which collect data under their own policies.

2.13 Data from others. We receive data from sign-in providers (2.1), payment providers (2.6), IP-intelligence and fraud services (2.7), and, if you use the community forum, from our forum provider ProductBridge.

3. How we use personal data and our legal bases

Purpose	Data used	Legal basis (EEA/UK)
Create and run your account, sign you in, provide plans and Credits	Account, session, billing data	Performance of our contract with you
Send your requests to Model Providers and return Output	Input, Output, usage metadata	Performance of contract
Charge for usage, enforce limits and queues, keep balances accurate	Usage and billing records	Performance of contract
Process payments, invoices, taxes and accounting	Payment and billing data	Contract; legal obligation
Prevent fraud, multiple-account abuse, rewards and refund abuse, and key theft	Session, IP, device fingerprint, payment risk signals, usage patterns	Legitimate interests in protecting the Service, our users and our payment relationships
Respond to chargebacks and payment disputes, and defend legal claims	Acceptance records, order, session, IP, device and usage records	Legitimate interests in defending our rights; legal claims
Secure the Service, investigate incidents and debug failures	Logs, error diagnostics (which may include request content, see 5.2)	Legitimate interests in operating a reliable, secure Service

Purpose	Data used	Legal basis (EEA/UK)
Enforce our Terms and Model usage policies, moderate image and video content	Media prompts and images, usage patterns, Coding Plan samples	Legitimate interests; legal obligation where reporting is required
Report child sexual abuse material and respond to lawful requests	Relevant account data and content	Legal obligation
Send service, security, billing and legal notices	Email, account data	Contract; legitimate interests
Send product updates and promotions you have not switched off	Email, preferences	Legitimate interests (existing customers) or consent where required; you can opt out at any time
Measure and improve our websites and Service	Analytics, aggregate usage	Consent where required for cookies; otherwise legitimate interests
Show ads that fund free Rewards	Ad-network data	Consent where required

Where we rely on legitimate interests, we have balanced them against your rights; you can object (Section 10). Where we rely on consent, you can withdraw it at any time without affecting earlier processing. Providing account and payment data is necessary to use the Service; if you do not, we cannot provide it.

Automated decisions. We use automated rules to detect fraud and abuse, for example to hold a first purchase for review when several risk signals match, to block suspected multiple accounts from free allowances, to suspend accounts linked to a payment dispute, and to slow Coding Plan traffic above fair-use levels. Some of these decisions can significantly affect you. These decisions are necessary to perform our contract with you and protect the Service (GDPR Article 22(2)(a)). You can obtain human review of any such decision, express your view and contest it by emailing support@electronhub.ai with the subject "Review".

4. Who we share personal data with

4.1 Model Providers. To fulfil a request we send its Input (and related metadata) to the Model Provider serving the chosen Model. Model Providers include model developers, cloud platforms, inference hosts, marketplaces, resellers and relay services, located in the United States, the European Union, China and other countries. **Each Model Provider processes your Input and Output under its own terms. Some keep it for a period, some may review it for abuse, and some, particularly providers of free or experimental endpoints, may use it to improve or train their models.** We do not control their practices, and a Model's displayed developer is not always the company that served the request (see Terms Section 3.2). We may also send parts of your conversation to helper Models we use for features such as conversation titles, tool calling on Models without native tool support, routing classification, web search and quality checks.

4.2 Service providers. We use providers that process data for us for hosting, databases, networking and security, sign-in and phone verification, payments, email and support, fraud and IP intelligence, content moderation, media hosting, network proxies, analytics and advertising, and the community forum. The current list, with what each does and where, is on the Subprocessors page.

4.3 Payment disputes. When you dispute a payment, we share the records described in Refund & Billing Policy section 7.3 with the payment provider, merchant of record, card network or bank handling the dispute.

4.4 Legal and safety. We disclose data when we believe in good faith that the law requires it, to respond to valid legal process, to report apparent child sexual abuse material to the National Center for Missing & Exploited Children or other authorities as the law requires, to protect the rights, safety or property of users, the public or us, or to enforce our Terms.

4.5 Business transfers. If we are involved in a merger, acquisition, financing, reorganisation or sale of assets, personal data may be transferred to the parties involved under confidentiality obligations.

4.6 Public content. Generated images are stored at publicly accessible URLs, images generated on the free plan or marked public may appear in a community gallery, and forum posts are public (Terms Section 8.6).

We do not sell personal information for money. See Section 11 for how California law treats analytics and advertising cookies.

5. Content we keep

We process your Input and Output to answer your requests and do not keep a standing copy of your conversations on our servers. Content is kept by us only in these cases:

5.1 Router cache (opt-in). If you turn on response caching in Router settings, we keep responses and a numerical representation of the last message for the time you choose (from 1 minute up to 30 days; 24 hours by default), only for your account.

5.2 Error diagnostics. When a request fails with an error other than a rate limit, we record diagnostic details to investigate it, which can include the full request content (messages, including earlier messages in the conversation, system prompt and tool definitions), the Model and provider, your user identifier, username and email, a masked key, IP address and country. These diagnostics are delivered to restricted internal channels used by our team (hosted on Discord) and are kept until our team deletes them. The same channels also receive payment and subscription events (with a masked email address and the provider's event data), sign-in failure details and abuse alerts.

5.3 Image generation. Prompts and resulting images for images generated on the free plan or marked public may be delivered to an internal or community gallery channel (hosted on Discord). Generated images are uploaded to public file hosting (Section 4.6). Image-generation requests made in chat may also be written to our application logs with your username and IP address.

5.3a Server logs. Our servers write operational logs that can include your username, a masked key, the route used and your IP address. These logs are kept by our hosting provider for its standard log period.

5.4 Coding Plan samples. Up to the 20 most recent prompt and response excerpts per Coding Plan key (Section 2.9).

5.5 Moderation and abuse. Content connected to a suspected violation, abuse investigation or legal report may be preserved as long as needed for that purpose or as the law requires.

6. International transfers

Our API servers run in the European Union (Germany), our main database is in the United States, and our providers and Model Providers operate in many countries, including the United States, the EU, the UK and China. When we transfer personal data from the EEA, UK or Switzerland to a country without an adequacy decision, we rely on safeguards such as the European Commission's Standard Contractual Clauses (and the UK addendum), the EU-

US Data Privacy Framework where the recipient is certified, or, where those are not available, the necessity of the transfer to perform our contract with you at your request (for example, sending your request to the Model you chose). You can ask us for information about the safeguards used.

7. How long we keep data

Data	Retention
Account and profile data	While your account exists; deleted when you delete it, except as below
Per-request usage logs (metadata, no content)	30 days, and at most the latest 1,000 entries per account
Daily usage totals and plan history	While your account exists
Lifetime usage totals per Model	Kept after account deletion in a form linked to your account identifier, for accounting and abuse prevention
Payment, order, refund and dispute records	Kept after account deletion for as long as tax, accounting and dispute rules require, generally up to 10 years
Transaction evidence: for each paid order, the order record; the versions of the Terms and Refund & Billing Policy accepted and the time, IP address and device of acceptance; IP addresses and device identifiers used at checkout and for sign-ins and API use from 30 days before to 120 days after the order; and daily usage and cost totals for that order's plan or keys	24 months after the order, or until any dispute, refund or legal claim about it is closed if later, including after account deletion

Data	Retention
Session records (IP, device, location)	Until the session expires, is revoked or the account is deleted
Fraud and abuse signals (device identifiers, IP counts, hashes of deleted emails)	While needed to prevent abuse; hashes of deleted emails may be kept indefinitely to prevent re-registration abuse
Coding Plan usage records	Usage up to 400 days; abuse signals 60 days; request samples and key records until the key is deleted
Router decision metadata	90 days (aggregate statistics up to 400 days)
Router pins	180 days after last use
Server logs (Section 5.3a)	Our hosting provider's standard log period
Notifications	90 days
Router cache (opt-in)	The period you choose, up to 30 days
Error diagnostics and image gallery items (Section 5)	Until deleted by our team
Generated images and uploaded avatars	Until you ask us to delete them; copies may remain with the host or third parties (Terms 8.6)

Data	Retention
Support messages	As long as needed to handle your request and related claims
Inactive free accounts	Free accounts with no paid plan, no permanent Credits and no activity for 90 days may be deleted
Content preserved for legal reports	As the law requires (for reports of child sexual abuse material, at least one year)

Account deletion. You can delete your account in the app. Deletion removes your account record, keys, sessions, notifications, rewards data, request logs and router data. Records listed above as kept after deletion, including transaction evidence, remain. Coding Plan records, MCP server settings, generated images and avatars are not removed automatically; email support@electronhub.ai to have them deleted. Deletion does not remove data stored in your browser; clear it in the app or your browser.

8. Security

We use industry-standard measures such as encryption in transit (TLS), hashing of session tokens, encryption of stored MCP OAuth tokens, access controls and monitoring. **The Service does not provide end-to-end encryption:** your requests are decrypted on our servers and sent to Model Providers so they can be processed. No system is completely secure. Keep your API keys and devices secure, and tell us at once if you suspect unauthorised access. If a personal-data breach is likely to put your rights at risk, we will notify the competent supervisory authority within 72 hours where required and tell affected users without undue delay.

9. Cookies and browser storage

We use a sign-in cookie, browser storage for the web app (your chats, workspace, memory, settings and API key are kept on your device), security cookies and device signals, and, on our websites, analytics and advertising cookies. The Cookie Policy lists them and explains your choices.

10. Your rights

Depending on where you live, you may have the right to:

- access your personal data and get a copy;
- correct inaccurate data;
- delete your data;
- restrict or object to processing, including processing based on legitimate interests and direct marketing;
- receive your data in a portable format;
- withdraw consent;
- not be subject to solely automated decisions with legal or similarly significant effects, and to obtain human review (Section 3);
- lodge a complaint with your data-protection authority.

To exercise your rights, email support@electronhub.ai from your account email, or use the account settings in the app. We may need to verify your identity. We respond within one month (extendable where the law allows), or within the time your local law requires. You can export your chats, workspace and memory from the web app at any time, because they are stored in your browser. If we refuse a request, we will explain why, and where your law provides an appeal, how to appeal.

11. United States privacy notice

This section supplements the Policy for residents of California and other US states with comprehensive privacy laws.

Categories collected in the last 12 months: identifiers (name, email, account and device identifiers, IP address); customer records and commercial information (plans, purchases, payment details from our processors); internet and network activity (usage records,

sessions, interactions with our websites); approximate geolocation (from IP); audio, electronic or visual content you submit; inferences used for fraud prevention; and sensitive personal information limited to account sign-in credentials and phone number, used only to provide and secure the Service. Sources, purposes and recipients are described in Sections 2 to 4, and retention in Section 7.

Sale and sharing. We do not sell personal information for money. Analytics and advertising cookies on our websites may count as "selling" or "sharing" for cross-context behavioural advertising under some state laws. To opt out, email support@electronhub.ai with the subject "Do not sell or share", block third-party cookies in your browser, or turn off personalised ads in your Google ad settings. We do not knowingly sell or share personal information of anyone under 16.

Your rights. You can request to know, access, correct and delete your personal information, to opt out of sale or sharing, and to limit the use of sensitive personal information (we only use it for permitted purposes). You may use an authorised agent. We will not discriminate against you for exercising your rights. Send requests to support@electronhub.ai.

12. Children

The Service is for adults aged 18 and over and is not directed to children. We do not knowingly collect personal data from anyone under 18. If you believe a child has given us personal data, contact us and we will delete it and close the account.

13. Changes to this Policy

We may update this Policy. We will post the new version with its effective date and, for material changes, notify you by email or in the app before they take effect.

14. Contact and complaints

Contact us at support@electronhub.ai. If you are in the EEA, UK or Switzerland, you may also complain to the data-protection authority where you live or work, or where an alleged infringement took place.