

Privacy Policy

Service: Kink IQ (incl. the ONYX co-pilot) **Effective:** June 30, 2026 **Last updated:** July 14, 2026

Version: 1.3

This policy explains what personal data Kink IQ collects, why, who we share it with, and the choices and rights you have. Because the Service is built around your relationships and intimate life, we treat that information as **sensitive by default** and only process it with care and on a lawful footing.

The short version

- We process information about your relationships, feelings, and intimate life only with your **explicit consent**, and only to provide the guidance and insight features you ask for.
- We use a third-party AI provider (**Anthropic**) to generate responses. Your inputs are sent to its API to produce replies. Under Anthropic's commercial API terms, this data is **not used to train AI models**.
- We **never sell** your personal data, and we do not use it for cross-context behavioral advertising.
- You can access, export, correct, or delete your data, and withdraw consent, at any time — see Your privacy rights.
- The Service is for adults **18 and older**. It is not therapy, medical, or mental-health care.

01 Who we are

Kink IQ (the "Service") is an AI communication co-pilot operated under the name **Kink IQ** ("we," "us," "our"). For data-protection purposes we are the **controller** of the personal data described in this policy.

You can reach our privacy team at butler@kinkiq.ai. A postal address for formal correspondence is available on request to the same address.

02 Scope & your role

This policy applies to Kink IQ and its website, app, and progressive web app at kinkiq.ai (together, the "Service"). It does not cover third-party services we link to, which have their own policies.

When you tell us about *other people* (for example, a partner or play partner you discuss with the ONYX co-pilot — including any private notes or partner profiles you choose to keep on them), you are responsible for that information. We store and process it **solely to provide the Service to you** — to power your co-pilot's memory and guidance. We do not contact those people, we do not build our own independent profiles of them for our own purposes, and we do not share your notes with anyone else. You can view, edit, or delete these notes at any time, and they are removed if you delete your account. This includes any **screenshots or images you upload** (for example, a chat thread or a profile): upload only images you are entitled to share, we store them solely to provide the Service to you, we transmit them to our AI provider to generate your read-out, and they are deleted when you delete the conversation or your account. Please only share information about others that you are entitled to share, and keep it to what you reasonably need for guidance.

03 Data we collect

We collect the following categories of personal data:

CATEGORY	EXAMPLES
Account data	Email address, display name, password (stored only as a salted hash), authentication tokens.
Profile & relationship data	Information you provide about yourself, your relationships, partners and play partners, dynamics, goals, and circumstances — including any private notes or partner profiles you keep, the scenes you log, and any screenshots or images you upload for ONYX to read.
Conversation & guidance content	The messages, prompts, profile text, scene details, and reflections you enter, and the AI responses ONYX generates for you.
Intimate / sensitive data	Details touching on your relationships, sexual orientation, or sex life that you choose to share — see Section 4.

CATEGORY	EXAMPLES
Payment data	Subscription tier, energy/credit balance, transaction history, and billing status, including a Stripe customer ID. Card details are collected and processed directly by Stripe ; we do not see or store full card numbers.
Usage & device data	Log data, approximate region (from IP), device/browser type, feature usage, and token ("energy") consumption, used for security, billing, rate limiting, and reliability.
Support data	Messages you send us and related correspondence.

You don't have to provide intimate or relationship data to create an account, but the core guidance features will not work without it.

04 Intimate & sensitive data

The Service is designed for you to discuss your relationships and intimate life. Some of what you share may reveal information that data-protection law treats as **special-category** or **sensitive personal data** — in particular data concerning your **sex life, sexual orientation, and the dynamics of your intimate relationships**.

OUR LEGAL BASIS FOR THIS DATA

Where this data falls within Article 9 of the GDPR, we rely on your **explicit consent** (Art. 9(2)(a)) to process it, which you give when you choose to enter such information into the Service. You can **withdraw consent at any time** (see Section 11); withdrawal does not affect processing already carried out, and may limit or end the guidance features.

We ask you not to share special-category data about *other people* unless you have a lawful basis to do so. We do not use sensitive data for advertising, and under US state law you have the right to limit our use of it (see Section 12).

05 How & why we use data

We use personal data for the purposes below, each with a lawful basis under Article 6 GDPR (and, for sensitive data, the Article 9 condition in Section 4):

PURPOSE	LAWFUL BASIS
Create your account and provide the Service's features	Performance of our contract with you (Art. 6(1)(b))
Process your relationship/intimate inputs to generate guidance and insight	Explicit consent (Art. 9(2)(a)); contract (Art. 6(1)(b))
Take payment and manage subscriptions	Contract (Art. 6(1)(b)); legal obligation for records (Art. 6(1)(c))
Keep the Service secure, prevent abuse, and debug	Legitimate interests (Art. 6(1)(f))
Improve and develop features using aggregated, de-identified usage and technical data only — never the content of your conversations or intimate data	Legitimate interests (Art. 6(1)(f))
Send service and (optional) marketing messages	Contract; consent for marketing (Art. 6(1)(a))
Comply with law and enforce our terms	Legal obligation (Art. 6(1)(c)); legitimate interests

We **do not use the content of your conversations, profile text, scene details, partner profiles, uploaded images, or any intimate data you share to improve or develop our features, and we do not use it to train AI models.** Product improvement relies only on aggregated, de-identified usage and technical data (for example, which features are used and error rates) that does not identify you or reveal what you shared.

Where we rely on legitimate interests, we balance those interests against your rights and you may object — see Section 11.

06 AI processing & Anthropic

The Service's advice and insight features (the ONYX co-pilot) are powered by a third-party large-language-model provider, **Anthropic**. When you use these features, the content you enter (which may include intimate or relationship data) is transmitted to Anthropic's API to generate a response, which is then returned to you.

- **No model training.** We use Anthropic's commercial API, under which your inputs and outputs are **not used to train Anthropic's models**.
- **Memory is for you only.** Information you save is used solely to provide personalised guidance, memory, and continuity within your own account. It is **never** used to build advertising profiles and is never shared with other users.
- **Current & future providers.** Anthropic is currently our primary AI provider. We may add other AI providers in future; if we do, we will list them in this policy before processing your data through them.
- **Sub-processor.** Anthropic acts as our sub-processor under a data-processing agreement and applies its own security and retention controls.
- **Sub-processor due diligence.** Before entrusting your data to a sub-processor, we assess whether its security, retention, and data-handling practices are appropriate to the sensitivity of that data, and we keep a record of that assessment. For transfers outside your region, we apply the safeguards described in the International transfers section below.
- **No solely-automated decisions with legal effect.** The Service provides suggestions, reflections, and information for *you* to consider and act on. We do not use it to make decisions about you that produce legal or similarly significant effects within the meaning of Article 22 GDPR.
- **AI outputs can be wrong.** Responses are generated by a model and may be inaccurate, incomplete, or unsuitable. They are not professional advice — see our Terms of Service.

07 Who we share data with

We do **not sell** your personal data. We share it only with the service providers (sub-processors) that help us run the Service, and only as needed:

PROVIDER	PURPOSE	REGION
Anthropic	AI generation of advisor responses (ONYX)	United States
Stripe	Payment processing & subscription billing	United States / global
DreamHost	Application hosting (VPS) and transactional email	United States
DreamObjects	Encrypted object/file storage	United States

We may also disclose data: to comply with law, legal process, or a lawful request; to protect the rights, safety, and security of users, the public, or us; and in connection with a merger, acquisition, or sale of assets, where the recipient is bound to honour this policy. We will tell you before your data becomes subject to a materially different

policy. We disclose personal data to government or law-enforcement bodies **only when legally required, or when necessary to protect the safety of our users or others**, and we push back on requests that are overbroad or unlawful.

We keep this sub-processor list current and publish material changes per Section 15.

08 International transfers

We and our sub-processors may process your data in countries outside your own, including the **United States**. Where we transfer personal data out of the European Economic Area, the United Kingdom, or Switzerland to a country without an adequacy decision, we rely on appropriate safeguards — principally the European Commission's **Standard Contractual Clauses** (and the UK International Data Transfer Addendum / Swiss addendum where relevant) — together with supplementary measures. You can request a copy of the relevant safeguards by contacting us.

09 How long we keep data

We keep personal data only as long as needed for the purposes in this policy, then delete or anonymise it. In general:

- **Account & profile data:** for the life of your account, then deleted within 30 days of account closure.
- **Conversation & guidance content:** until you delete it or close your account, subject to the same 30-day deletion window.
- **Payment & tax records:** as long as required by law (commonly up to 7 years).
- **Logs & security data:** up to 12 months.
- **Backups:** deleted information may persist in encrypted backups for a limited period (typically up to 30 days) before being permanently overwritten.

We may retain limited data longer where necessary to comply with law, resolve disputes, or enforce our agreements.

10 Security

Your data is stored on encrypted servers located in the **United States**. We use technical and organisational measures appropriate to the sensitivity of the data, including encryption in transit (TLS), encryption at rest for stored content, hashed passwords, access controls, and least-privilege practices. We also keep access logs and

monitor for unauthorised access. No system is perfectly secure, but we work to protect your data and will notify you and any regulator of a personal-data breach where the law requires (under the GDPR, within 72 hours of becoming aware, where the threshold is met).

11 Your privacy rights

Depending on where you live, you have some or all of these rights over your personal data:

- **Access** — get a copy of the data we hold about you.
- **Rectification** — correct inaccurate or incomplete data.
- **Erasure** — have your data deleted ("right to be forgotten").
- **Portability** — receive your data in a portable format.
- **Restriction & objection** — limit or object to certain processing, including processing based on legitimate interests and any direct marketing.
- **Withdraw consent** — where we rely on consent (including for intimate/sensitive data), withdraw it at any time without affecting prior processing.

You can **delete your account at any time** from within the app (Account → Delete my account) or by contacting us, and you can **export your data** from the app; exports are provided in a common machine-readable format (JSON). To exercise any other right, contact butler@kinkiq.ai or use the in-app privacy controls. We respond within the time the law requires (generally one month under the GDPR). We will not charge you or treat you differently for exercising your rights, except as the law allows.

If you are in the EEA, UK, or Switzerland and believe we have mishandled your data, you may complain to your local data-protection supervisory authority.

12 US state privacy rights

If you are a resident of California or another US state with a comprehensive privacy law, you have additional rights, which may include the right to know, access, correct, and delete your personal information; to opt out of "sale" or "sharing" of personal information; to limit the use of **sensitive personal information**; and to be free from discrimination for exercising your rights.

- **We do not sell your personal information**, and we do not "share" it for cross-context behavioral advertising, as those terms are defined under California law.
- You may exercise the right to **limit the use of sensitive personal information** by contacting us; we already restrict its use to providing the Service and related operations.

- You may use an authorised agent to submit requests, subject to verification.

To exercise these rights, contact butler@kinkiq.ai. California residents may also request information under California's "Shine the Light" law.

13 Children & age (18+)

The Service is intended only for adults aged **18 or older**. We do not knowingly collect personal data from anyone under 18, and the Service is not directed to children. If you are under 18, do not use the Service or provide us any information.

If we learn that we have collected personal data from anyone under 18, we will delete it promptly. If you believe a minor has provided us data, contact butler@kinkiq.ai.

14 Cookies & tracking

We use cookies and similar technologies that are strictly necessary to run the Service (for example, to keep you signed in) and, with your consent where required, a limited set for analytics to improve reliability. We do not use advertising or cross-site tracking cookies. You can control non-essential cookies through your browser settings.

15 Changes to this policy

We may update this policy as the Service or the law changes. We will post the updated version here with a new "Last updated" date, and for material changes we will give you reasonable notice (for example, by email or in-app notice) before they take effect. Where the law requires, we will seek your renewed consent.

This policy is governed by the law identified in our Terms of Service, subject to any mandatory data-protection rights you have where you live.

16 Contact us

Questions, requests, or complaints about this policy or your data:

Kink IQ

Web: kinkiq.ai

Email: butler@kinkiq.ai

Postal address available on request.