

# Faceless Launchpad — Privacy Policy

**Effective date:** 12/09/2025

**Entity / Controller:** Faceless Launchpad, operated by **Ascentir Management Consultancies FZCO** (Dubai, United Arab Emirates) (“**Faceless Launchpad**,” “**we**,” “**us**,” “**our**”).

**Scope:** This Policy explains how we collect, use, disclose, and protect personal data in connection with our programs and digital offerings (including online courses, 1-on-1 mentorship, community access, events, templates, and related materials) sold or provisioned via Whop or our checkout pages (collectively, the “**Programs**”).

If you use the Programs, you agree to this Privacy Policy, our **Terms of Service** and **Refund & Dispute Policy**.

## 1) Data we collect

We collect personal data you provide directly, data generated through your use of the Programs, and limited data from third parties.

- **Identity & Contact:** name, email, country/region, company, handle/username.
- **Account & Auth:** login identifiers, hashed passwords, MFA tokens, role/permissions.
- **Transactional:** order IDs, purchase history, payment status, last 4 of card (via processor), amounts, currency, taxes; **we do not store full payment card numbers.**
- **Program Use:** course progress, quiz results, downloads, portal/community activity, messages you post, submissions/homework, support tickets.
- **Coaching & Events:** registrations, attendance, **session recordings** (audio/video/screen/name/avatar/chat).
- **Technical & Logs:** IP address, device/browser type, time zone, language, referrer, cookie IDs, session timestamps, error/fraud signals.
- **Communications & Marketing:** preferences, email engagement (opens/clicks), survey responses, testimonials (with your consent for public use).
- **Introductions to Freelancers (if requested):** the minimum contact/project info necessary to facilitate an introduction.
- **From Third Parties:** payment processors, authentication providers, analytics tools, and the platform used to provision Programs (e.g., Whop/LMS/community providers) may send us limited data necessary to operate your account.

## 2) Why we process your data (purposes) & legal bases

We process personal data only where we have a legal basis (examples below reflect GDPR/UK GDPR):

- **Provide & operate the Programs** (create accounts, deliver content, schedule sessions, support) — *Contract necessity*.
- **Payments & billing** (process orders, prevent duplicate charges, receipts, tax) — *Contract necessity / Legal obligation*.
- **Anti-fraud, abuse prevention & platform security** (rate-limiting, anomaly detection, enforcing acceptable use) — *Legitimate interests*.
- **Dispute/chargeback defense & legal claims** (maintain evidence, respond to payment network requests) — *Legitimate interests*.
- **Program improvement & analytics** (usage measurements, feature performance, QA, research) — *Legitimate interests*.
- **Marketing with your consent** (emails about updates, offers; you can opt out anytime) — *Consent / Legitimate interests* for existing customers where permitted.
- **Compliance** (court orders, sanctions screening, bookkeeping) — *Legal obligation*.

## 3) How we use recordings and community content

Group calls, webinars, and some 1-on-1 sessions may be **recorded** for replays, training, quality assurance, dispute defense, and to support those who could not attend. By attending, you consent to recording. If you prefer, keep your camera off and use a display name. Do **not** share or upload replays publicly.

Community spaces are moderated. Do not post sensitive personal data. We may remove or restrict content that violates our rules.

## 4) Cookies & similar technologies

We (and our service providers) use cookies, local storage, and similar technologies to keep you logged in, remember preferences, measure performance, and secure the Programs. You can manage cookies in your browser and (where offered) via our cookie banner. Disabling some cookies may limit functionality.

## 5) How we share information

We do **not** sell personal data. We share it only with:

- **Service providers / processors** that help us operate the Programs (hosting, LMS, community/chat, email service, analytics, customer support, authentication, video conferencing, storage, and **payment processors**).
- **Freelancers you ask us to contact** (limited details necessary for an introduction).
- **Payment networks, banks, platforms** (e.g., Whop) as required to process transactions, fight fraud, or resolve disputes/chargebacks.
- **Legal & safety:** regulators, courts, law enforcement, or others where required by law or to protect rights, safety, or enforce Agreements.
- **Corporate events:** in a merger, acquisition, or asset sale, data may transfer under this Policy's protections.

We require processors to protect data, use it only per our instructions, and implement appropriate security.

## 6) International transfers

We operate from the **UAE** and may process data in the UAE, the **EEA/UK**, the **United States**, and other locations where our providers are based. Where required (e.g., EEA/UK → non-EEA), we use appropriate safeguards such as **Standard Contractual Clauses** or other lawful transfer mechanisms.

## 7) Data retention

We keep personal data only as long as necessary for the purposes described above, including:

- **Account & Program records:** for your access term and a reasonable period afterward to manage re-enrollment and support.
- **Transactions, tax & bookkeeping:** typically **6–10 years** (subject to applicable law).
- **Security & access logs / dispute evidence:** for our anti-fraud controls and **defense of legal claims** (commonly up to **6 years**, or longer if litigation is reasonably anticipated).
- **Recordings:** for the access term and a reasonable period for replays, QA, and dispute defense.  
When data is no longer needed, we delete, anonymize, or securely store it offline where required by law.

## 8) Your rights

Depending on your location, you may have rights to:

- **Access** a copy of your personal data.
- **Rectify** inaccurate or incomplete data.
- **Erase** (delete) data in certain circumstances.
- **Restrict** or **object** to certain processing (including processing based on legitimate interests).
- **Portability** (receive your data in a structured, commonly used format).
- **Withdraw consent** where processing is based on consent (e.g., marketing).
- **Lodge a complaint** with your local supervisory authority (e.g., an EU/EEA Data Protection Authority or the UK ICO).

To exercise rights, email [hello@facelesslaunchpad.com](mailto:hello@facelesslaunchpad.com) with your request and the email used for your account. We may verify your identity before acting. Some rights may be limited by law (e.g., we may retain records needed for legal, tax, fraud-prevention, or dispute-defense purposes).

## 9) Children

Our Programs are for adults **18+** (or the age of majority in your jurisdiction). We do not knowingly collect personal data from children. If you believe a child provided data, contact us and we will take appropriate steps.

## 10) Security

We use administrative, technical, and physical safeguards appropriate to the nature of the data and risks involved (access controls, encryption in transit, least-privilege, logging/monitoring, backups, employee confidentiality). No system is perfectly secure; you are responsible for safeguarding your credentials and using unique, strong passwords with MFA where available.

## 11) Marketing preferences

You can opt out of marketing emails at any time by clicking “unsubscribe” or emailing [hello@facelesslaunchpad.com](mailto:hello@facelesslaunchpad.com). We may still send **transactional or service** messages (e.g., purchase confirmations, critical notices).

## 12) Automated decisions

We do not engage in solely automated decision-making that produces legal or similarly significant effects about you. We may use automated signals to detect fraud/abuse and to prioritize support.

## 13) Third-party links & tools

The Programs may link to third-party sites or integrate third-party tools (e.g., payment providers, community platforms, analytics). Their privacy practices are governed by their own policies. Review those policies before using third-party services.

## 14) Jurisdiction-specific disclosures

- **EEA/UK:** Our primary legal bases are **contract necessity**, **legitimate interests**, **consent**, and **legal obligation**. For international transfers, we use recognized safeguards (see §6). You may lodge complaints with your local DPA/ICO.
- **California (CPRA):** We do **not** sell or share personal information for cross-context behavioral advertising. You may exercise access, deletion, and correction rights by emailing [hello@facelesslaunchpad.com](mailto:hello@facelesslaunchpad.com). We verify and respond per CPRA timelines.

## 15) Changes to this Policy

We may update this Policy from time to time. When we do, we will revise the “Effective date” and, if changes are material, provide additional notice (e.g., at checkout or via email/portal). Your continued use of the Programs after changes take effect constitutes acceptance.

## 16) Contact

Questions, requests, or complaints about privacy: [hello@facelesslaunchpad.com](mailto:hello@facelesslaunchpad.com)  
Business: Faceless Launchpad — Ascentir Management Consultancies FZCO, Dubai, UAE.  
If you are in the EEA/UK and believe your rights were not respected, you can also contact your local supervisory authority.