

# Lussa Privacy Policy

## 1) Who we are and how to contact us

This Privacy Policy explains how Lussa (“Lussa”, “we”, “us”, “our”) handles personal data when you use our websites, game(s), creator tools, marketplace, esports/community programs, and related services (the “Services”).

**Controller:** Visionarie Labs Technology Services LLC, trading as Lussa, and (where applicable) its regional affiliates that provide the Services in your country.

**Contact:** [privacy@lussa.io](mailto:privacy@lussa.io)

**EU/UK representatives:** Where required by Article 27 GDPR/UK GDPR, Lussa has appointed H. Batuhan as its EU/UK representative who can be contacted at [privacy@lussa.io](mailto:privacy@lussa.io).

## 2) Scope

This Policy applies to personal data we process about:

- Players, creators, and developers using our game and creator tools
- Marketplace buyers/sellers (via our payment partners)
- Community members (forums/Discord), esports/ambassador applicants and participants, university-program participants, and website visitors
- Business contacts (publishers, studios, partners, vendors)

## 3) Personal data we collect

We collect the following categories of personal data (depending on your use of the Services):

- **Account & profile:** name/username, email, password, age or age-band, country, preferred language, display/avatar information.
- **Gameplay & platform activity:** in-game identifiers, session data, progress, achievements, inventory/assets, anti-cheat and integrity signals, crash/diagnostic logs.

- **UGC & communications:** creations, posts, comments, reports, and (if enabled) voice/text chats; content flagged for moderation.
- **Device & technical:** IP address, device IDs, OS/browser info, settings, approximate location (from IP), performance metrics, cookies/SDKs, and similar technologies.
- **Payments & transactions:** purchase history, refunds, marketplace listings, and limited payment metadata; full payment card data is handled by our PCI-compliant payment processors.
- **Community/esports/university programs:** application form data (e.g., name, university/faculty, role, social handles, country), eligibility and participation data.
- **Marketing preferences:** newsletter opt-ins, campaign interactions, and events RSVPs.
- **Support & safety:** support tickets, reports, enforcement records, and appeal outcomes.

## 4) Sources

- Directly from you (account setup, forms, purchases, UGC, support)
- Automatically from your device and Services usage (see Cookies/SDKs)
- From partners providing hosting, payments, anti-cheat, analytics, moderation, or login federation (e.g., platform SSO)
- Public data you make available (e.g., public profiles) where permitted

## 5) How we use your data and our legal bases (EU/UK)

We use your data to:

- **Provide and secure the Services** (create/manage accounts; deliver gameplay, UGC tools, marketplace and tournament features; anti-cheat; DDoS prevention; bug-fixing). *Legal bases: contract; legitimate interests; legal obligation.*
- **Moderation & safety** (detect harmful content/behavior, enforce rules, prevent fraud/abuse). *Legal bases: legitimate interests; legal obligation.*

- **Payments & marketplace** (fulfill purchases, prevent fraud, handle refunds/taxes). *Legal bases: contract; legal obligation; legitimate interests.*
- **Analytics & service improvement** (performance, balancing, feature usage). *Legal bases: legitimate interests; consent where required for cookies/SDKs.*
- **Communications** (service messages; optional newsletters/events). *Legal bases: contract; legitimate interests; consent where required.*
- **Marketing & personalization** (non-essential cookies/SDKs; first-party recommendations). *Legal bases: consent where required; otherwise legitimate interests with opt-out.*
- **Esports/community/university programs** (review applications, eligibility, event ops). *Legal bases: contract; legitimate interests; consent where required.*
- **Legal compliance** (tax, accounting, regulatory requests, rights handling). *Legal bases: legal obligation.*

Where we rely on **consent** (e.g., non-essential cookies, certain marketing, or processing of precise location where applicable), you can withdraw it at any time in the product settings or via our cookie banner.

## 6) Cookies, SDKs, and similar technologies

We use:

- **Strictly necessary** (security, fraud prevention, load balancing)
- **Functional** (preferences, remembering settings)
- **Analytics** (aggregate usage, performance)
- **Advertising/marketing** (only where permitted and with required choices)

In the EU/UK, we'll only set non-essential cookies/SDKs with your consent under ePrivacy/PECR; you can change choices anytime via "Cookie Settings." In the US, we provide opt-out where cookies/SDKs constitute a "sale" or "share" or "targeted advertising" under applicable state laws, including honoring **Global Privacy Control (GPC)** signals where required.

## 7) When we share data

We share personal data with:

- **Service providers / processors** (hosting, storage/CDN, security/anti-cheat, moderation, analytics/measurement, product feedback, CRM, support, email/SMS, payments/tax)
- **Commercial partners** (platform integration partners; esports/university partners—only for the relevant program and with appropriate safeguards)
- **Authorities** (law enforcement or regulators when legally required)
- **Corporate transactions** (M&A, financing, or reorganization, subject to confidentiality and continued protection)

We do **not** sell your personal information in the conventional sense. Where our use of ad/analytics tech could be interpreted as a “sale,” “share,” or “targeted advertising” under US law, you can opt out (see Section 12).

## 8) International transfers

We operate globally and use vendors in several countries. When transferring personal data internationally, we use:

- **EU/EEA → US:** the **EU-US Data Privacy Framework (DPF)** for certified providers, or the **2021 Standard Contractual Clauses (SCCs)** with transfer impact assessments.
- **UK → US:** the **UK Extension to the DPF** for certified providers, or the **UK IDTA/Addendum** with SCCs.
- Other regions: equivalent contractual or legal mechanisms as required.

## 9) Retention

We keep personal data only as long as needed for the purposes above, including legal, tax, and accounting requirements, then delete or de-identify it. Retention varies by data category (e.g., account records for the life of the account + a limited period; payments per statutory periods; safety logs for a shorter rolling window).

## 10) Security

We use administrative, technical, and organizational safeguards appropriate to the risks (including encryption in transit, access controls, network security, and anti-abuse tooling). No system is 100% secure; we maintain and test controls and have incident response procedures.

## 11) Your rights

**EU/UK:** access; rectification; erasure; restriction; portability; objection; withdrawal of consent; and the right to lodge a complaint with your DPA/ICO.

**US (state laws):** right to know/access, correction, deletion, portability, and the right to **opt out** of sale/share/targeted advertising; some states grant the right to **limit** the use/disclosure of sensitive personal information and require recognition of **UOOM** (e.g., GPC). See Section 12 for how to exercise. (US state privacy laws vary; we apply a consistent rights experience across covered states.)

**Exercising rights:** Email [privacy@lussa.io](mailto:privacy@lussa.io) or use in-product tools where available. We may verify your request and, where allowed, respond through an authorized agent.



## 12) US State Notice at Collection

We provide this summary of the categories we collect, purposes, retention, and whether we “sell” or “share” PI (as those terms are defined by law):

Category of PI	Examples	Business/Commercial Purposes	Retention	Sold/Shared?*
Identifiers	name, email, username, device IDs, IP	account, security, support; service comms; fraud/abuse	life of account + legal	<b>No sale; Share</b> for ads/analytics only with opt-out
Customer records	purchase history	fulfill transactions, tax, fraud	statutory retention	<b>No sale; No share</b>
Internet/activity	gameplay telemetry, logs, cookie/SDK data	security, performance, analytics; personalization/ads (where allowed)	rolling windows tuned to need	<b>No sale; Share</b> possible with opt-out
Geolocation (coarse)	IP-derived region	content delivery, fraud	short rolling	<b>No sale/share</b>
UGC / comms	creations, posts, reports, chat (if enabled)	publish features; moderation/safety	life of account or shorter safety windows	<b>No</b>
Inferences (limited)	interest segments	product improvements; personalization	short rolling	<b>Share</b> possible with opt-out
Sensitive PI (rare)	precise location, government IDs— <b>not collected</b> for consumers; payment card handled by processors	N/A	N/A	N/A

\*“Share” refers to cross-context behavioral advertising; you can **opt out** at any time via the “Do Not Sell or Share My Personal Information / Opt-out of Targeted Ads” link in the footer and we honor **Global Privacy Control (GPC)** signals where applicable.

## 13) Children

The Services are **not directed to children under 13** (or the age required in your country). We do not knowingly collect personal data from children without appropriate consent. If you believe a child has provided personal data, contact [privacy@lussa.io](mailto:privacy@lussa.io) and we'll delete it as required. We follow COPPA in the US and the UK Children's Code principles where relevant to teen audiences. (If we later release teen-focused features, we will implement age-appropriate safeguards before launch.)

## 14) Third-party services

We integrate with hosting, anti-cheat, moderation, analytics/measurement, and payments. Their use of data is governed by their privacy terms; we contractually require adequate protections and transfer mechanisms.

## 15) Automated decision-making / profiling

We may use automated systems for security (e.g., anti-cheat/fraud) and to recommend content. You can contact us to learn more and, where required by law, request human review.

## 16) Appeals (US)

If we decline to act on a US state privacy request, you may appeal by replying to our decision email. We will respond to appeals within 45 days, extendable once by 45 days where reasonably necessary. If you remain dissatisfied, you may contact your state Attorney General.

## 17) Changes to this Policy

We'll update this Policy when needed. If changes materially affect your rights, we'll provide prominent notice (e.g., in-product or email). Your continued use after the effective date means you accept the updated Policy.

## 18) Contact

Email: [privacy@lussa.io](mailto:privacy@lussa.io) Postal: FAO: H. Batuhan Cetin Visionarie Labs Technology Services LLC's at Al Saaha Offices B, 404, Souk Al Bahar, Burj Khalifa Station, Dubai, UAE.