Global Privacy Policy

(for visitors and users of https://link2app.site and related services)

Effective date: 20 October 2025

Service Name: link2app.site
Contact for privacy matters: privacy@link2app.site
Postal address: 25 Rustaveli Ave, Batumi 6010, Georgia

Data Controller: Not appointed
EU Representative (GDPR Art. 27): Not appointed
UK Representative (UK GDPR Art. 27): Not appointed
Data Protection Officer (DPO): Not appointed

> This Policy explains what personal data we collect, why we collect it, the legal bases we rely on, how we share and transfer data internationally, how long we keep it, your rights, and how to exercise them. Regional Addenda at the end provide jurisdiction-specific notices.

1) Scope

This Policy applies to all websites, apps, and integrations of link2app.site where it is posted or referenced. By using our services, you acknowledge this Policy.

2) Key terms

- **Personal Data:** any information relating to an identified or identifiable natural person.
- **Processing:** any operation performed on Personal Data (collection, storage, use, disclosure, etc.).
- **Controller:** the party determining purposes and means of processing.
- **Processor:** a party processing Personal Data on behalf of a Controller.
- **International transfer:** sending Personal Data outside your jurisdiction.

3) Data we collect

Depending on your use of the service, we may collect:

- **Identification & contact data:** name, email, account identifiers.

- **Communications:** support messages, requests, feedback.
- **Technical & usage data:** IP address, device/browser type, referrers, visited pages/events, cookie IDs, SDK event logs.
- **Payment-related data:** tokens/identifiers from payment providers and transaction status (we do not store full card details; certified processors handle payment credentials).
- **Marketing & analytics signals:** page views/clicks, UTM tags, ad network IDs, consent/opt-in or opt-out choices.

4) Sources

- **Directly from you:** account sign-up, forms, communications.
- **Automatically:** cookies, SDKs, logs generated by your device/browser.
- **Third parties:** payment processors, analytics, and integration partners where lawful and necessary.

5) Purposes and legal bases

We process data to:

- **Provide and support the service** (including personalization and account features).
- **Ensure security and prevent fraud,** debug and monitor performance.
- **Perform analytics and improve the product.**
- **Conduct marketing with consent** where required (e.g., emails, retargeting).
- **Comply with legal obligations** and **protect our rights/interest** where applicable.

GDPR/UK GDPR legal bases (as applicable): performance of a contract; **legitimate interests** (e.g., security, limited analytics with minimal impact); **consent** (for non-essential cookies/marketing); **legal obligation;** vital interests (where relevant). You may object to processing based on legitimate interests where your interests override ours.

6) Cookies & SDKs

We use:

- **Strictly necessary cookies** (core functionality).

- **Functional/analytics cookies** (product improvement, aggregated statistics).

- **Marketing/advertising cookies** (used only with consent where required).
  You can manage cookies in your browser and via our banner/preferences center (where available). We honor **Global Privacy Control (GPC)** signals in jurisdictions that require it (e.g., California).

7) Sharing of Personal Data

We share data only as needed:

- **Processors/service providers:** hosting, support, analytics, email delivery, payments—bound by data processing terms and our instructions.

- **Partners/integrations:** at your request or with your consent.

- **Compliance and law enforcement:** where required by law.

- **Corporate transactions:** mergers, acquisitions, or asset transfers—with notice where required.

We **do not sell** your Personal Data for money. See the U.S. section for “Do Not Sell/Share” under CPRA.

8) International transfers

When Personal Data is transferred across borders, we apply appropriate safeguards, such as:

- **EU Standard Contractual Clauses (SCCs)** with supplementary measures, and **UK Addendum** for UK transfers.

- **EU-U.S./UK-U.S. Data Privacy Framework (DPF)** where the U.S. recipient is certified.

- **Transfer impact assessments** where required.
  You may request information about these safeguards at privacy@link2app.site.

9) Retention

We retain Personal Data only as long as necessary for the purposes described here or as required by law/contract. Typical periods: active accounts — for the life of the account; logs — short operational periods; financial records — as required by applicable law. After expiry, data is deleted or anonymized.

10) Security

We implement technical and organizational measures (encryption in transit, access controls, monitoring). No method of transmission or storage is 100% secure.

11) Automated decision-making

We do not make decisions producing legal or similarly significant effects solely by automated means without appropriate safeguards, unless permitted by law.

12) Your rights and how to exercise them

Depending on your location, you may have rights to **access, rectify, delete, restrict, port, object,** withdraw consent, lodge a complaint with a regulator, and **not be discriminated against** for exercising rights.
How to request: email **privacy@link2app.site**. We may ask for identity verification. We respond within legally required timelines (typically 30–45 days).

13) Children

Our services are not directed to children under the applicable age of consent (**EU/EEA: 13–16 depending on the Member State; U.S.: under 13 under COPPA**). We do not knowingly collect such data. If you believe a child provided data, contact us to delete it.

14) Changes to this Policy

We may update this Policy from time to time. The “Effective date” above will change accordingly. Where required, we will provide additional notice (e.g., banner or email).

15) Contact & complaints

Questions and requests: **privacy@link2app.site**.
You may also complain to your local data protection authority (e.g., an EU supervisory authority; UK ICO; Brazil ANPD; Canada OPC; Australia OAIC; Singapore PDPC; South Africa Information Regulator).

Regional Addenda

A) EU/EEA & UK (GDPR/UK GDPR)

- **Controller:** Not appointed.
- **EU/UK Representatives:** Not appointed.

- **Legal bases:** contract; legitimate interests (security, improvements, limited analytics); consent (non-essential cookies/marketing); legal obligation.

- **Your rights:** access; rectification; erasure; restriction; portability; objection (including to marketing and to processing based on legitimate interests); withdrawal of consent; complaint to a supervisory authority.

- **International transfers:** SCCs/UK Addendum with supplementary measures; DPF where applicable.

B) United States (e.g., California CPRA; Virginia, Colorado, Connecticut, Utah, Texas, etc.)

- **State privacy rights:** know/access; correct; delete; data portability; **opt-out** of "sale" or **"sharing"** for cross-context behavioral advertising; limit use/disclosure of **sensitive personal information**; appeal a denied request (where applicable).

- **Do Not Sell/Share:** we do not sell Personal Data for monetary consideration. Under CPRA, "sharing" can include using advertising cookies for cross-context ads—you may **opt out** via our banner/preferences center and/or by sending a **GPC** signal, which we honor for California residents.

- **Notice at Collection:** we collect identifiers (email, cookie/ad IDs), internet activity (page views/events), approximate geolocation (city/country level), and inferences for personalization, for the purposes in Sections 5–7. Sources: you, your device, and service providers. Retention: see Section 9.

C) Brazil (LGPD)

- **Legal bases:** contract; legitimate interest; consent; legal obligation; credit protection where applicable.

- **Rights:** confirmation of processing; access; correction; anonymization/blocking/deletion; portability; information on sharing; withdrawal of consent; complaint to **ANPD**.

D) Canada (PIPEDA)

- We process data under principles of fairness, purpose limitation, and proportionality.

- **Rights:** access and correction; complaints to the **Office of the Privacy Commissioner of Canada (OPC)**.

E) Singapore (PDPA)

- **Rights:** access; correction; withdrawal of consent; portability (if applicable). Complaints: **PDPC**. We maintain reasonable security arrangements.

F) Australia (Privacy Act)

- We follow the Australian Privacy Principles (APPs): notice, purpose limitation, data quality/security, access/correction. Complaints: **OAIC**.

G) South Africa (POPIA)

- Principles: lawfulness, minimality, purpose limitation, transparency.
- **Rights:** access, correction, objection, complaint to the **Information Regulator**.

Third-party services and payments

Payments and certain features are provided by third-party providers acting as processors or, in limited cases, independent controllers. Their terms and privacy policies apply in addition. A list of key providers and compliance statuses (e.g., PCI DSS, DPF) is available on request.

How to reach us

For any privacy question or to exercise your rights, email **privacy@link2app.site**. We aim to respond within the timelines required by your local law.