FutureSelf Mobile App Privacy Policy

Last Modified: September 19, 2025

Introduction

FutureSelf, owned and operated by Lurra, LLC (“**FutureSelf**,” “**Company**,” “**we**,” “**us**,” or “**our**”) respects your privacy and is committed to protecting it. This Privacy Policy explains:

- The types of information we collect when you download, install, register with, access, or use the FutureSelf mobile application (the “**App**”).

- Our practices for collecting, using, maintaining, protecting, and disclosing that information.

Scope. This policy applies only to information we collect **in the App** and in email, text, and other electronic communications sent in connection with the App. It **does not** apply to information collected offline, on websites or apps not controlled by FutureSelf, or by any third party (see **Third-Party Information Collection**). Those sites/apps have their own privacy policies.

By downloading, registering with, or using the App, you agree to this Privacy Policy. If you do not agree, do not use the App. We may update this policy from time to time (see **Changes to This Policy**).

Definitions

- **“Outputs”** means the AI-generated or AI-transformed images the App produces at your direction from your inputs, including single images, “before & after” composites, comparison-slider frames, thumbnails, previews, blurred or watermarked versions, and any technical derivatives (e.g., resized, compressed, or cached renderings) delivered to your device. **Outputs exclude** the App, models, software, prompts/templates provided by us, and any training data.

- **“Vision Board”** means the local (on-device) area of the App where you may choose to save Outputs and your progress photos.

- **“User Content”** means content you submit or generate in the App (e.g., your uploaded photos, progress photos, and, when saved locally by you, Outputs).

For EU/UK privacy law purposes, **Lurra, LLC d/b/a FutureSelf** is the **data controller** for processing described in this policy.

Individuals Under the Age of 18

The App is **not intended for children under 18**, and we do not knowingly collect personal information from anyone under 18. If we learn we have collected personal information from a child under 18, we will delete it. If you believe we might have information from or about a child under 18, contact **team@microgramapp.com**. (Additional rights for California residents under 16 may apply—see **Your State Privacy Rights**.)

Information We Collect and How We Collect It

We collect information **from and about** users:

- **Directly from you** when you provide it.
- **Automatically** when you use the App.

A. Information You Provide

Depending on the features you use, you may provide:

- **Account & demographics:** email (optional if/when accounts are supported), **gender**, **age group**, **body goal** (e.g., build muscle / lose weight).
- **Photos you upload** to generate Outputs (see **Sensitive Data & Photos**).
- **Progress photos** and locally saved **Outputs** on your device.
- **Support** communications (e.g., emails you send us).
- **Purchase/subscription details** as provided by your platform provider (e.g., Apple). We do **not** receive your full payment card details; platform providers process payments.

You may also submit information for in-App features that evolve over time. If you post or share content outside the App (e.g., to social apps), that use is governed by those third parties.

B. Information Collected Automatically

When you access or use the App, we may automatically collect:

- **Usage details/events:** session counts/timestamps; feature interactions (e.g., upload/generation/unlock events); in-App notifications; referral/attribution data.

- **Device & diagnostics:** device type, operating system and version, App version/build, language/locale, crash/performance logs, approximate IP-based region.

- **Subscription status:** active/canceled, renewal dates, and related platform confirmations.

If you prefer not to share this information, do not use the App or adjust device settings where available (note: some data are necessary to provide core functionality and security).

C. Third-Party Information Collection

When you use the App or its content, certain **third parties** may collect information about you or your device, including:

- **App stores and payment processors** (e.g., purchases, renewals, refunds).

- **Analytics and diagnostics providers** (e.g., app performance, crashes).

- **AI processing providers** (to generate your Outputs).

- **Attribution/marketing partners** (where used, consistent with your device permissions).

We do not control these third parties' tracking technologies or how they may be used. Their practices are governed by their own privacy policies. Questions about an advertisement or targeted content should be directed to the responsible provider.

Sensitive Data & Photos (Explicit Consent)

Certain data you provide may be considered **sensitive** under applicable law (e.g., photos of your body, weight- or body-related imagery). FutureSelf:

- **Does not perform facial recognition** and does **not** attempt to identify individuals in images.

- **Processes images ephemerally** via **third-party AI providers** solely to generate your **Outputs** and for safety/moderation and abuse prevention.

- **Does not permanently store** uploaded or generated images on our servers. If you choose to save, images and Outputs are saved **locally on your device** (and may be included in your device/OS backups if you enable them).

Your Consent (Required for Core Functionality). Because generating Outputs requires processing **images of your body that we treat as sensitive personal data (e.g., "special-category data" under EU/UK law)**, **we can only provide the core Service if you give explicit consent**. If you do not consent, please do not use the App. If you withdraw consent, the App's core features will no longer function and you should stop using and delete the App. Withdrawing consent does not affect the lawfulness of processing carried out before withdrawal. We may retain minimal records as required by law (e.g., purchase/transaction records, security logs). Images and Outputs saved **locally on your device** remain under your control; delete them (and any OS/device backups) if you stop using the App.

How to withdraw. In **Settings → Privacy**, you can turn off **Photo Processing** (which disables uploads/generation going forward) and **Delete local images & Outputs**.

Data Minimization

We collect the **minimum** data needed to operate, secure, and improve the App. Specifically, we store **only**: gender, age group, body goal, and operational/diagnostic metrics described above. We **do not** collect biometric identifiers and **do not** perform facial recognition. Where feasible, metrics are aggregated and/or de-identified.

How We Use Your Information

We use information to:

- **Provide and operate** the App (generation of Outputs via third-party AI providers, safety/moderation, in-App paywall and unlock, Vision Board).
- **Maintain security**, prevent fraud and abuse, and enforce our **Terms of Service**.
- **Process subscriptions** and communicate about your account (e.g., renewal notices).
- **Improve** the App, including analytics, diagnostics, and performance.
- **Comply with legal obligations** and respond to lawful requests.
- **Communicate** with you about updates, changes, and support.

We **do not** use your images to train our **own** models. Third-party AI providers may have their own policies regarding retention or model improvement—see **Disclosures** and **International Transfers**.

Legal Bases for Processing (EEA/UK Users)

Where GDPR/UK GDPR applies, our legal bases include:

- **Explicit consent (required for core functionality).** To generate Outputs we process **images of your body**, which we treat as **sensitive personal data** (“special-category data”). We can provide the core Service **only if you give explicit consent**. If you **do not consent**, please do not use the App. If you **withdraw consent**, the App’s core features will no longer function and you should stop using and **delete the App**. Withdrawing consent does **not** affect the lawfulness of processing carried out **before** withdrawal.

- **Contractual necessity.** We process limited, non-sensitive data (e.g., subscription status, device/app version, necessary account details) to provide the Service you request, maintain access control, and handle billing/renewals.

- **Legitimate interests (non-sensitive data only).** We process operational analytics, diagnostics, and security/anti-abuse signals to operate, secure, and improve the App—balanced against your rights and expectations.

- **Legal obligation.** We may process/retain limited information to comply with laws (e.g., tax, accounting, fraud prevention, lawful requests).

Disclosures of Your Information

We may disclose:

- **To service providers/processors** who help us operate the App, including: hosting/infrastructure, analytics/diagnostics, crash reporting, attribution/marketing (where used), **AI processing providers** (to generate Outputs), and customer support tools. These providers process information under their own terms and privacy policies, which may include their independent retention or use of data as described by them. We do not control their practices; please review their privacy policies.

- **To platform providers** (e.g., app stores/payment platforms) for purchases, renewals, and refunds.

- **For legal reasons:** to comply with law, regulation, legal process, or governmental request; to enforce our Terms; to protect the rights, safety, and security of users, us, or the public.

- **Corporate transactions:** in connection with a merger, acquisition, financing, or sale of assets, subject to appropriate safeguards.
- **With your direction or consent.**
- **Aggregated/de-identified data** that does not identify you may be shared without restriction.

Local-only images. We do **not** store images server-side; images saved on your device or in your OS backups are under your control (and your OS/provider's control where applicable).

International Data Transfers

International Transfers. We and our service providers (including cloud hosting and **AI Processing Providers**) may process personal information in countries outside your own (e.g., the United States). Where EU/UK law applies, we rely on approved transfer safeguards—such as the European Commission's **Standard Contractual Clauses**—as made available by our vendors, and, where applicable, other frameworks. Additional details are available in our vendors' privacy/compliance documentation.

Retention

We retain personal information **only as long as necessary** for the purposes described above, including operating the App, complying with legal obligations, resolving disputes, and enforcing agreements. Images/Outputs saved locally remain on **your device** until you delete them (or your OS backup policy removes them).

Data Security

We employ administrative, technical, and organizational measures designed to protect personal information (e.g., encryption in transit, access controls, and logging). No method of transmission or storage is 100% secure; use of the App is at your own risk. You are responsible for safeguarding device access, credentials, and any backup settings. We do not permanently store uploaded or generated images on our servers; if you save images, they are stored locally on your device and may be included in OS/device backups you control.

Your Rights

A. EEA/UK Data Subject Rights

Subject to exceptions, you may have the right to **access**, **rectify**, **erase**, **restrict**, **object**, and **port** your personal data, and to **withdraw consent** at any time (without affecting prior processing). You also have the right to lodge a complaint with your local data protection authority.

To exercise rights, contact **team@microgramapp.com**. We may request information to verify your identity and respond within the time required by law.

B. U.S. State Privacy Rights (e.g., CA/VA/CO/CT/UT)

Residents of certain U.S. states may have rights to **access**, **delete**, **correct**, **port**, and to **opt-out** of certain data "sales" or "sharing" and targeted advertising, as defined by applicable law. We do **not** sell personal information as "sale" is commonly defined, and we do not use images for targeted advertising. You can submit a request at **team@microgramapp.com**. We will not discriminate against you for exercising your rights.

If we deny your request, you may **appeal** by replying to our response or emailing team@microgramapp.com with "Appeal" in the subject line. We will inform you of the outcome and how to contact your state authority, where applicable.

Choices & Controls

- **Device permissions.** You may disable camera/photos permissions at any time in your device settings (some features will not function).
- **Local deletion.** You may delete saved images/Outputs from the App's Vision Board and your device/OS backups if desired.
- **Marketing.** If we send marketing emails, you can unsubscribe via the link in the email. Transactional/service emails will still be sent.

Do Not Track

Do Not Track. The App does not respond to "Do Not Track" (DNT) signals. Mobile platforms provide their own privacy controls (e.g., iOS App Tracking Transparency, Android advertising settings), which we honor where applicable.

Third-Party Links and Services

The App may include links to third-party sites/services. Their privacy practices are governed by their own policies; we are not responsible for their content or practices.

Changes to This Policy

We may update this Privacy Policy from time to time. If we make **material** changes, we will post the updated policy in the App and/or otherwise notify you as required. The "Last Modified" date indicates the latest update. Continued use of the App after changes means you accept the updated policy.

Contact Us

Lurra, LLC d/b/a FutureSelf
367 St. Marks Ave, Brooklyn, NY 11238, USA
Email: team@microgramapp.com

How to Contact Authorities

If you have concerns about our handling of personal data, you may contact your local **Data Protection Authority** (EEA), the **UK Information Commissioner's Office (ICO)**, or your **state privacy authority**.
