



Privacy Policy

Last Updated: July 2026

1. Data We Collect and Process..... 3

2. How We Secure Your Data..... 3

3. Third-Party Processors..... 4

4. Data Retention & UK GDPR Compliance..... 4

We are committed to safeguarding the privacy of our users while maintaining transparent data management workflows. This Privacy Policy outlines how your information is securely held, processed, and transmitted when you interact with our AI architecture.

1. Data We Collect and Process

- **Account Information:** To manage session tokens and ledger balances, we collect and store your session token and basic account metrics (such as your user ID, available credit tiers, and billing transaction log history) inside our database infrastructure.
- **User Media and Input Data:** We process the images you upload (e.g., room photos, blueprint layouts, facade captures) and the text prompts you submit.
- **Audit and Diagnostic Metadata:** To maintain operational security and prevent credit fraud, our backend automatically generates immutable audit logs containing your user ID, action type, module endpoint, execution success status, final credit changes, and prediction IDs.
- **Contact Information:** Your email address and optional name are collected when you create an account for communication and account recovery.
- **Device and Access Logs:** To maintain service security and operational performance, we collect your IP address, browser type, device type, and access timestamps.
- **Payment Information:** If you purchase credits, payment processing is handled by our payment processor (Stripe). We do not store your full payment card details
- **Cookies and Tracking:** Our platform uses essential cookies (for session tokens and security) which are strictly necessary to operate the service. We also use statistical analytics tools (such as Google Analytics) solely to measure aggregated service usage, track website traffic, and improve website functionality. Under UK law, these statistical cookies do not require prior active consent. However, you have the right to object to their use at any time. You can opt out of analytics tracking by using the official [Google Analytics Opt-out Browser Add-on] or by emailing us at support@koros.space with your request.

2. How We Secure Your Data

- **Data in Transit:** When you upload images, they are transmitted to us over encrypted HTTPS connections. Your upload or generated images are stored in isolated cloud storage buckets (Cloudflare R2) with restricted access.
- **Access Control:** When your images are sent to AI processing services (e.g. Replicate, Modal), we generate temporary access links. This prevents permanent public access to your uploads.
- **Logging:** To detect fraud and maintain system health, we log user actions (what you uploaded, when, result success/failure) but we do NOT store full image copies in our audit logs — only metadata about the request.

- **Data Minimisation:** Raw images are usually cleared from temporary processing layers within 24 hours of use. See Section 4 for retention periods.

However, we cannot guarantee perfect security. If you are concerned about uploading sensitive property photos or client work, consider using anonymized references or placeholder images.

3. Third-Party Processors

To execute design tasks, we transmit your User Content (images, prompts) to the following third-party processors. You are responsible for reviewing their privacy policies before uploading sensitive content:

- **Replicate.com (California, USA) & Black Forest Labs (BFL)**
 - Processes: Images for image transformations, generation, furniture and content detection.
 - Retention: Images sent to these third-party processors for active generation are permanently deleted from their servers within 24 hours of processing. Request logs are retained for up to 30 days.
 - Link: <https://replicate.com/privacy>
- **Modal.com (California, USA)**
 - Processes: GPU compute tasks for image segmentation
 - Retention: GPU memory is cleared immediately after job completion
 - Link: <https://modal.com/privacy>
- **Stripe Inc. (California, USA) -**
 - Processes: Payment card details, billing address, transaction history -
 - Retention: Per Stripe's policy (typically 7 years for PCI compliance) -
 - We do NOT store your full card number; Stripe tokenizes it - Link: <https://stripe.com/privacy>
- **International Data Transfers & AI Infrastructure:**
 - Our backend routing utilizes cloud infrastructure and specialized GPU clusters provided by Replicate, Inc. and Modal Labs, located in the United States. When you upload media or submit design prompts, this data is transferred outside the UK/EEA for serverless inference execution. We ensure these transfers are protected via standard contractual safeguards, and these providers maintain strict data minimization workflows (including automated temporary data deletion protocols within 60 minutes of execution)
 - For users outside the USA, data is transferred internationally. We rely on the UK International Data Transfer Agreement (IDTA) or the UK Addendum to the EU Standard Contractual Clauses, as recognised by the UK Information Commissioner's Office (ICO), to ensure adequate protection equivalent to UK GDPR standards
 - You are responsible for ensuring that any User Content you upload does not infringe third-party IP rights or violate local laws. If your use of a third-party processor's output results in claims, Koros Space is not liable for third-party breaches or policy changes beyond our control.
- **AI Training Policy:**

- Koros Space strictly does not use your personal data, uploaded photos, or generated blueprints to train our own proprietary AI models. However, we utilise third-party infrastructure (such as Replicate and Black Forest Labs) to process your design requests. These third-party processors may collect and use prompts, input images, and generated outputs to develop, test, or train their own foundational models in accordance with their respective privacy policies. We encourage you to review their specific terms before uploading highly sensitive or proprietary imagery.

4. Data Retention & UK GDPR Compliance

Data Control: You are the data subject. Koros Space is the data controller under UK GDPR Article 4. We process your data lawfully under the basis of:

- **Contract:** Providing the design generation service you've requested
- **Legitimate Interest:** Fraud detection, system security, abuse prevention

Retention Periods:

- **Account & Billing Data** (email, credit ledger, transaction history): Retained for 7 years after account closure (to comply with UK tax requirements and potential disputes).
- **Uploaded Images & Generated Outputs (User Content):** Images you upload and the design outputs generated by our platform are safely stored on Koros Space servers for as long as your account remains active. This ensures you have uninterrupted access to your project history and blueprints. If you delete a specific project or render from your dashboard, the associated images are immediately and permanently removed from our active servers.
- **Audit Logs** (user actions, success/failure, credit changes): Retained for 90 days for fraud detection and customer support. Older logs are anonymized.
- **Analytics Data** (Google Analytics, if enabled): Retained per Google's policy (typically 26 months). You can opt out in Settings → Privacy.
- **Cookies:** Session cookies expire when you log out. Analytics cookies expire per your browser settings.

Account Deletion & Data Erasure: You have the right to completely delete your Koros Space account and all associated personal data, uploaded images, and generated renders at any time.

- **How to delete:** You can instantly delete your account directly through your **Account Settings / Dashboard**, or by emailing **support@koros.space**.
- **What happens:** Upon deletion, all of your user content (images, blueprints, and outputs) is permanently purged from our servers.

- **Exceptions:** Legal holds (such as active fraud investigations, payment disputes, or legal proceedings) or our mandatory 7-year retention for billing and transaction records may delay the deletion of specific financial and administrative data by up to 90 days.

Your Data Rights under UK GDPR:

- Right of Access (Article 15): You can request a copy of all personal data we hold about you.
- Right to Rectification (Article 16): You can correct inaccurate data (email, name, billing address).
- Right to Erasure (Article 17): You can request deletion of your account and data, except where:
 - Legal holds require retention (fraud investigation, payment disputes)
 - 7-year accounting records must be kept
 - Processing is necessary for contract fulfilment
- Right to Data Portability (Article 20): You can request your account data in machine-readable format (CSV/JSON) for import to another service.
- Right to Object (Article 21): You can object to processing for fraud detection or analytics. Fraud detection is mandatory; analytics can be disabled in Settings.
- Right to Restrict Processing (Article 18): You can request we freeze processing while you dispute data accuracy.

To invoke any of these rights, or to submit a formal data protection complaint, please email support@koros.space. In accordance with the Data (Use and Access) Act 2025, we will formally acknowledge receipt of your complaint within 30 days and investigate the matter without undue delay. If you remain dissatisfied with our resolution, you retain the right to lodge a complaint with the UK Information Commissioner's Office (ICO) at ico.org.uk.

Right to Lodge a Complaint: If you believe we've violated your privacy rights, you can lodge a complaint with the UK Information Commissioner's Office (ICO) at ico.org.uk.

5. Data Breach Notification

In the unlikely event of a security breach affecting your personal data, we will:

- Notify you within 24 hours of discovery (via email to your account address)
- Inform the UK ICO within 72 hours if the breach poses high risk to your rights
- Provide details of: what data was accessed, who was affected, what steps you should take

If you believe a breach has occurred, contact support@koros.space immediately.

6. Updates to This Privacy Policy

We reserve the right to update this policy to comply with new regulations or improve our services. Material changes (e.g., changes to data retention, third-party processors, or your rights) will be notified to you via email at least 30 days before taking effect. Continued use of the Platform after the change date constitutes acceptance.