Data Processing Agreement

Last updated: February 2026

This Data Processing Agreement ("DPA") forms part of the agreement between you ("Controller") and KoalaPic ("Processor") for the use of KoalaPic's image conversion services via the API. This DPA is entered into pursuant to Article 28 of the General Data Protection Regulation (EU) 2016/679 ("GDPR").

1. Definitions

- **Controller:** The entity (the API user's organization) that determines the purposes and means of processing personal data by using KoalaPic's services.
- **Processor:** KoalaPic, which processes personal data on behalf of the Controller when performing image conversion, compression, and metadata extraction services.
- **Personal Data:** Any data relating to an identified or identifiable natural person, including images containing faces, EXIF metadata (GPS coordinates, device information, timestamps), IP addresses, and email addresses associated with API accounts.
- **Processing:** Any operation performed on personal data, including upload, format conversion, compression, metadata extraction, temporary storage, transmission, and deletion.
- **Sub-processor:** Any third party engaged by KoalaPic to process personal data on behalf of the Controller.
- **Data Subject:** The individual whose personal data is processed, including persons depicted in uploaded images and API account holders.

2. Scope of Processing

Purpose

KoalaPic processes personal data solely to perform image format conversion, compression, and metadata extraction as instructed by the Controller via API requests.

Types of Personal Data

- Images, which may contain faces, text, or location-identifiable content
- EXIF and GPS metadata embedded in image files
- File names, which may contain personal identifiers
- IP addresses of API callers
- Email addresses of API account holders

Categories of Data Subjects

- End users whose images are uploaded for conversion
- API account holders who operate the integration

Duration

Processing occurs only for the duration of the conversion. Uploaded and converted files are automatically deleted within 1 hour of conversion completion. Temporary files are cleaned every 15 minutes. Conversion metadata (format, file size, timestamps — no image content) is retained for up to 30 days for anonymous users and indefinitely for authenticated users until account deletion.

Nature of Processing

All processing is fully automated. No human review of uploaded images occurs. Each conversion runs in an isolated task with no cross-user data access.

3. Obligations of the Processor

KoalaPic, as Processor, commits to the following obligations:

- **Processing on instructions only:** Process personal data only on documented instructions from the Controller. The API request parameters (format, quality, resize, metadata handling) constitute the Controller's instructions.
- **Purpose limitation:** Not process data for any purpose other than performing the requested conversion, compression, or metadata extraction.
- **Confidentiality:** Ensure that persons authorized to process personal data are bound by appropriate confidentiality obligations.
- **Security measures:** Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, as detailed in Section 5 of this DPA.
- **Sub-processor restrictions:** Not engage additional sub-processors without the Controller's prior consent, as detailed in Section 6.
- **Data subject rights assistance:** Assist the Controller in responding to data subject requests for access, rectification, erasure, and portability, as detailed in Section 9.
- **Deletion after processing:** Delete all personal data after the end of processing. Image files are automatically deleted within 1 hour. Account data is deleted upon request via the self-service dashboard or API.
- **Audit and compliance:** Make available all information necessary to demonstrate compliance with GDPR Article 28 obligations. Allow for and contribute to audits and inspections conducted by the Controller or an authorized auditor.

4. Obligations of the Controller

The Controller is responsible for:

- Ensuring a lawful basis exists for processing personal data through KoalaPic (e.g., consent, legitimate interest, contractual necessity)
- Informing data subjects that their data may be processed by KoalaPic as a sub-processor, where required by applicable law
- Not uploading data that is prohibited under KoalaPic's Terms of Service, including illegal content, malware, or child exploitation material
- Providing instructions to KoalaPic that comply with applicable data protection laws
- Ensuring that any personal data submitted for processing is adequate, relevant, and limited to what is necessary for the intended conversion

5. Technical and Organizational Measures

KoalaPic implements the following security measures to protect personal data:

- **Encryption in transit:** All data is transmitted over TLS 1.2 or higher. HTTPS is enforced via HTTP Strict Transport Security (HSTS) with preload.
- **Encryption at rest:** Server disk encryption is enabled on all storage volumes.
- **Access control:** API key authentication with SHA-256 hashed key storage. No plain-text API keys are retained after initial generation. Keys are prefixed with kp_ for identification without exposure.
- **Data minimization:** Uploaded and converted files are automatically deleted within 1 hour of conversion completion. Temporary files are cleaned every 15 minutes. Maximum upload size is 50 MB per file.
- **Network security:** Content Security Policy (CSP) with nonce-based script sources, Cross-Origin Resource Sharing (CORS) restrictions, and CSRF protection on browser-facing API requests. Rate limiting with progressive abuse escalation and automatic IP-level banning.
- **Input validation:** All uploaded files are validated by magic byte verification (not just file extension), MIME type checking, file size limits (50 MB), SVG script sanitization, and decompression bomb protection.
- **Monitoring:** Application error logging, automated health checks, and Sentry error tracking for operational monitoring. No image content is sent to monitoring systems.
- **Isolation:** Each conversion runs as an isolated background task. There is no cross-user data access between conversion operations.
- **Backup and recovery:** Database backups with point-in-time recovery for metadata only. Image files are ephemeral and not included in backups.

6. Sub-processors

KoalaPic uses the following sub-processors:

Sub-processor	Purpose	Data Processed
Infrastructure Provider	Server hosting, compute, storage	All data processed by KoalaPic
Cloudflare	CDN, DDoS protection, Turnstile CAPTCHA	Web traffic metadata. No image data for API requests.
Sentry	Error monitoring	Error context and stack traces only. No image content.

KoalaPic will notify the Controller of any intended changes to sub-processors by updating the DPA page and providing reasonable opportunity to object. The Controller may object to a new sub-processor by contacting support@koalapic.com within 30 days of notification.

7. International Data Transfers

KoalaPic's primary servers are located in the European Union. Where personal data is transferred outside the European Economic Area (EEA), appropriate safeguards are in place:

- Cloudflare and Sentry may process limited operational data (error reports, traffic metadata) in the United States. Both maintain their own Data Processing Agreements and rely on Standard Contractual Clauses (SCCs) and/or adequacy decisions for international transfers.
- No image content is transferred to sub-processors outside the EEA.
- If the Controller is located outside the EEA, data transfers to KoalaPic's EU servers are covered by Standard Contractual Clauses, available upon request.

8. Data Breach Notification

KoalaPic will notify the Controller without undue delay, and in any event within 72 hours, after becoming aware of a personal data breach affecting the Controller's data. The notification will include:

- The nature of the breach, including the categories and approximate number of data subjects affected
- The likely consequences of the breach
- The measures taken or proposed to address the breach and mitigate its effects
- The name and contact details of the point of contact for further information

Security concerns should be reported to security@koalapic.com.

9. Data Subject Rights

KoalaPic assists the Controller in fulfilling data subject rights as follows:

- **Right of access and portability:** Authenticated users can retrieve their conversion metadata via the API (GET /api/v1/conversions). Image files are not retained beyond 1 hour and cannot be retrieved after deletion.

- **Right to erasure:** Authenticated users can delete their account and all associated data via the account settings dashboard or the API (DELETE /api/v1/account). Anonymous conversions are automatically deleted within 1 hour.
- **Right to restriction and objection:** The Controller should contact KoalaPic at support@koalapic.com to restrict or cease processing for specific data subjects.

10. Term and Termination

- This DPA is effective for the duration of the Controller's use of KoalaPic's services.
- Upon termination, KoalaPic deletes all Controller's data. File data is automatically deleted within 1 hour of conversion. Account data is deleted upon account closure.
- This DPA survives termination of the main Terms of Service to the extent necessary to fulfill data deletion obligations.

11. Governing Law and Jurisdiction

This DPA is governed by the same law and jurisdiction as the main Terms of Service. The GDPR applies to the processing of personal data of data subjects in the European Union and European Economic Area, regardless of the governing law of this agreement.

12. How to Execute This Agreement

This DPA is effective when the Controller uses KoalaPic's API services. By generating an API key and making API requests, the Controller accepts the terms of this DPA.

For a countersigned copy of this agreement, contact support@koalapic.com.

Last updated: February 2026