



archyl

Data Processing Agreement

GDPR-compliant data processing addendum for Archyl services

Version 3.0 • September 27, 2026

Classification: Public

EKO Consulting • EURL • SIRET 842 435 547 00026 • France

1. Definitions

- **"Personal Data"** means any information relating to an identified or identifiable natural person as defined in Article 4(1) of the GDPR.
- **"Processing"** means any operation or set of operations performed on Personal Data, as defined in Article 4(2) of the GDPR.
- **"Data Subject"** means the identified or identifiable natural person to whom the Personal Data relates, as defined in Article 4(1) of the GDPR.
- **"Sub-processor"** means any processor engaged by the Processor to carry out specific processing activities on behalf of the Controller.
- **"GDPR"** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).
- **"Controller"** means the natural or legal person which determines the purposes and means of the processing of Personal Data, as defined in Article 4(7) of the GDPR.
- **"Processor"** means a natural or legal person which processes Personal Data on behalf of the Controller, as defined in Article 4(8) of the GDPR.

2. Scope and Purpose

This DPA applies to the processing of Personal Data by Archyl (the Processor) on behalf of the Customer (the Controller) in connection with the following activities:

- Providing the Archyl architecture documentation platform
- User account management and authentication (including MFA)
- Team collaboration features
- Storage of user-uploaded documentation file attachments
- AI-powered architecture discovery, AI chat and coding agents (when enabled)
- Transactional e-mail (invitations, verification, password reset, notifications)
- Customer support services

3. Data Processing Details

Subject Matter	Processing of Personal Data for architecture documentation services
Duration	For the term of the service agreement plus data retention period
Nature & Purpose	Storage, retrieval, and processing of architecture documentation and collaboration data
Data Categories	User identifiers, email addresses, authentication tokens, MFA secrets, user-generated content (including uploaded file attachments)
Data Subjects	Customer's employees, contractors, and authorized users

4. Processor Obligations

4.1 Processing Instructions

- Process Personal Data only on documented instructions from the Controller
- Immediately inform the Controller if any instruction infringes applicable data protection law
- Ensure persons authorized to process Personal Data are bound by confidentiality obligations

4.2 Security Measures

The Processor shall implement and maintain appropriate technical and organizational measures including:

- Application-level encryption at rest of credentials and customer content (AES-256-GCM, Argon2id-derived key), and encryption in transit (TLS 1.3)
- Encryption of uploaded file attachments at rest (AES-256) in private object storage, served via short-lived signed URLs
- TOTP-based Multi-Factor Authentication with single-use challenges and encrypted recovery codes
- Single sign-on (SAML 2.0, OIDC) with browser-bound, single-use state
- Role-based access controls enforced per resource, with automated tenant-isolation tests
- JWT authentication with configurable expiry and server-side session revocation
- Rate limiting on login, MFA, password-reset, public and webhook endpoints
- Protection against server-side request forgery on all customer-configurable integrations
- Security event logging for authentication failures and access denials
- Automated vulnerability and secret scanning in CI/CD (govulncheck, CodeQL, gitleaks, Trivy)
- Regular internal penetration testing, with findings remediated and regression-tested
- Hardened containers: non-root, read-only root filesystem, dropped capabilities, pinned dependencies
- Incident detection and response capabilities via Sentry and Prometheus
- Data backup and recovery procedures

4.3 Sub-processing

- Not engage another processor without prior written authorization
- Maintain a list of approved sub-processors (see Section 6)
- Notify the Controller at least 30 days before any intended changes to sub-processors
- Ensure sub-processors are bound by equivalent data protection obligations
- Remain liable for sub-processor compliance

4.4 Data Subject Rights

- Assist the Controller in responding to data subject requests
- Provide functionality for data export (/users/me/export) and full cascade account deletion
- Respond to requests within legally required timeframes

5. Controller Obligations

- Ensure lawful basis for processing Personal Data
- Provide clear instructions regarding data processing
- Inform data subjects about data processing activities
- Handle data subject requests and complaints
- Conduct data protection impact assessments where required

6. Approved Sub-processors

Sub-processor	Purpose	Location	Safeguards
Google Cloud Storage	Object storage for documentation file attachments (Archyl Cloud)	EU (Belgium) / configurable	SCCs, ISO 27001, SOC 2/3. Self-hosted deployments may use any S3-compatible provider

Sub-processor	Purpose	Location	Safeguards
OpenAI	AI analysis (optional)	USA	SCCs, DPA. Self-hosted Ollama available as alternative
Mailgun	Transactional e-mail delivery	USA / EU	SCCs, SOC 2. Self-hosted deployments may use their own SMTP server
Stripe	Payment processing	USA (EU data center)	SCCs, PCI-DSS Level 1
Sentry	Error tracking & monitoring	USA / EU	SCCs, SOC 2, GDPR compliant
GitHub	OAuth authentication & repo access	USA	SCCs, SOC 1/2, ISO 27001
GitLab	OAuth authentication & repo access	USA / EU	SCCs, SOC 2, ISO 27001
Bitbucket	OAuth authentication & repo access	USA / EU	SCCs, SOC 2, ISO 27001

Sub-processor Updates

- The Controller will be notified of any intended changes to sub-processors at least 30 days before the change. The Controller may object to changes within this period.

7. Security Measures

7.1 Technical Measures

Measure	Implementation
Encryption at Rest	AES-256-GCM with per-operation random nonce, Argon2id key derivation
Object Storage	Private S3-compatible buckets (Google Cloud Storage on Archyl Cloud), AES-256 at rest, signed-URL access
Encryption in Transit	TLS 1.3 for all communications, database SSL required
Access Control	Resource-bound RBAC, OAuth 2.0, SAML/OIDC SSO, JWT with session revocation, TOTP MFA, scoped API keys (read-only by default)
Network Security	Localhost-only service binding, CORS, Content-Security-Policy, SSRF-safe outbound client, HTTP timeouts
Input Validation	go-playground/validator, parameterized SQL queries, size limits
Monitoring	Structured JSON logging, security event logging, Sentry alerting, Prometheus metrics
Container Security	Non-root (UID 10001), read-only root filesystem, dropped capabilities, seccomp, checksum-verified build tools
Security Testing	CI scanning (govulncheck, CodeQL, gitleaks, Trivy) and recurring internal penetration tests

7.2 Organizational Measures

- Security policies and procedures documentation
- Employee confidentiality agreements
- Incident response procedures
- Vendor security assessments
- Quarterly internal security reviews and penetration testing

8. Data Breach Notification

8.1 Notification Requirements

- Notify the Controller without undue delay, within 72 hours (GDPR Article 33)
- Provide all information required for Controller to comply with breach notification obligations
- Take immediate steps to contain and remediate the breach

8.2 Notification Content

- Nature of the breach including categories and number of affected data subjects
- Contact details for further information
- Likely consequences of the breach
- Measures taken or proposed to address the breach

9. Data Retention and Deletion

9.1 During the Agreement

- Personal Data retained for the duration necessary to provide services
- Security event logs retained ~90 days (Docker log rotation: 50MB x 30 files per service)
- Architecture change history retained for the duration of the project

9.2 Upon Termination

- Customer may export all data before account termination via `/users/me/export`
- Upon request, all Personal Data will be deleted within 30 days via full cascade account deletion
- Uploaded file attachments are removed from object storage when their documentation, or the account, is deleted
- Backup copies deleted according to retention schedule (maximum 30 days)
- Deletion certificate available upon request

10. International Transfers

- Primary data storage region configurable via `SERVER_DATAREGION`
- Default: EU (Belgium, europe-west1) — including the object-storage bucket for file attachments

Where data is transferred outside the EU/EEA, the following safeguards apply:

- Standard Contractual Clauses (SCCs) with all non-EU sub-processors
- Transfer Impact Assessments conducted for each sub-processor
- Supplementary measures implemented where required

11. Audits and Inspections

- Make available all information necessary to demonstrate compliance
- Allow for and contribute to audits conducted by the Controller or an auditor

- Provide audit reports and certifications upon request

Audit Process

- Audit requests should be submitted with at least 30 days notice. Third-party audit reports may be provided as an alternative where available.

12. Liability

- Each party shall be liable for damages caused by processing that infringes this DPA or GDPR
- The Processor shall be liable for damages caused by its sub-processors
- Liability caps as set out in the main Terms of Service apply

13. Term and Termination

- This DPA is effective upon acceptance of the Terms of Service
- This DPA terminates upon termination of the service agreement
- Provisions regarding data deletion and return survive termination

14. Contact Information

Data Protection Inquiries	Security Incidents
privacy@archyl.com	security@archyl.com
Response: Within 5 business days	Response: Within 24 hours

Document Control

Version	3.0
Effective Date	September 27, 2026
Classification	Public
Owner	Archyl Legal Team

Legal Entity

- **Company Name:** EKO Consulting
- **Legal Form:** EURL (Entreprise Unipersonnelle à Responsabilité Limitée)
- **SIRET:** 842 435 547 00026
- **Country:** France

End of Data Processing Agreement v3.0