Automwrite

DATA SECURITY AND COMPLIANCE OVERVIEW

Automwrite Ltd – Data Security & Compliance Overview

1. Data Hosting & Residency

Primary hosting: Amazon Web Services (AWS) in eu-west-2 (London, UK).

Production environment: All production data, backups, and disaster-recovery replicas remain within the UK/EU region.

Data transfers: Personal data may be transmitted to approved sub-processors solely for service delivery purposes, including natural-language processing (OpenAI OpCo, LLC and Anthropic PBC), authentication (Clerk.com, Inc.), payment processing (Stripe, Inc.), and transcription services (AssemblyAI, Inc.). All transfers occur over encrypted channels (TLS 1.2+).

Transfer safeguards: Sub-processors execute Data Processing Agreements incorporating Standard Contractual Clauses where required for international transfers. We assess sub-processor privacy and security posture during onboarding and upon material changes.

Data minimisation: Requests to sub-processors transmit only the minimum data fields necessary for service delivery. System and user messages sent for language processing contain contextual information required for generating letters but exclude unnecessary direct identifiers where technically feasible.

2. Security Controls

Encryption in transit: TLS 1.2+ enforced for all external communications and API integrations. All sub-processor connections use HTTPS.

Encryption at rest: AWS-managed encryption applied to S3 object storage and automated backups.

Identity & access management:

- Multi-factor authentication available via Clerk authentication platform for user accounts
- Role-based access control (RBAC) enforced at the application layer
- API key authentication available with BCrypt hashing (strength 12)
- Least-privilege principle applied to AWS IAM policies
- API key usage tracked with timestamp and request count

Logging & monitoring:

- AWS CloudWatch monitoring for infrastructure and application metrics
- Alerting for critical system events
- Application logs retained for operational purposes
- API key usage tracking maintained for security auditing

Business continuity: AWS RDS automated backups with point-in-time recovery capability stored in-region (eu-west-2).

3. Data Governance & Roles

Controller vs processor: Customers are data controllers; Automwrite Ltd acts as a data processor on customers' behalf.

Registration: Automwrite Ltd is registered with the UK Information Commissioner's Office (ICO registration 00011727535).

Data Protection Impact Assessments: We conduct privacy assessments for AI-assisted processing activities as part of our ongoing compliance program.

Data subject rights: Requests (access, rectification, deletion, restriction, portability, objection) handled via help@automwrite.co.uk with acknowledgement within 2 business days and resolution within 30 calendar days as required by UK GDPR.

4. Access Management

Customer controls: Organisation administrators manage user provisioning, role assignment, and access revocation through the application interface.

Internal access: Role-based access controls enforced at the application layer. Authentication is performed via JWT token validation or API key authentication. Authorisation checks verify permissions for each action after authentication. Privileged operations (e.g., organisation deletion, user management) are restricted to authorised users only.

Auditability: API key usage logged. Authentication events and privileged actions tracked.

5. Incident Response & Breach Notification

Monitoring: AWS CloudWatch monitoring with real-time alerting for system anomalies and critical errors. Documented incident response procedures maintained.

Response targets:

- Critical incident triage: Within 4 business hours of alert during UK business hours; 24-hour response for after-hours alerts
- Containment actions: Within 24 hours of confirmed incident
- Customer notification: Within 72 hours of confirming a personal-data breach

Communication: Dedicated incident channel (help@automwrite.co.uk) plus out-of-band messaging if primary systems impaired.

Regulatory reporting: UK ICO and relevant supervisory authorities notified within 72 hours of becoming aware of qualifying personal data breaches, per UK GDPR Article 33.

6. Data Retention & Deletion

In-life deletion:

- Users can delete their accounts and associated personal data via the application interface
- Organisation owners can delete entire tenants, which cascades to all dependent data including: user accounts, clients, letters, templates, organisation settings, chat histories, and S3-stored files

- Deletion executes immediately unless retention is required by legal or regulatory obligations

Data exports: Data exports available via help@automwrite.co.uk within 7 calendar days.

7. Sub-Processors

Current sub-processors:

- AWS EMEA SARL - Cloud infrastructure hosting
- OpenAI OpCo, LLC - Language model processing for letter generation
- Anthropic PBC - Language model processing for letter generation
- Clerk.com, Inc. - User authentication and identity management
- Stripe, Inc. - Payment processing
- AssemblyAI, Inc. - Audio transcription services

We apply data minimisation principles to all AI requests, excluding unnecessary direct identifiers where technically feasible. All LLM sub processors are GDPR and Data Protection compliant.

8. Support & Contact

- Technical support: daniel.braghis@automwrite.co.uk (business hours UK time)
- Security & privacy inquiries: lusine.tumoyan@automwrite.co.uk
- Emergency contact: +44 7885 582656