Automwrite – Data Security and Compliance Overview

1. **Data Storage and Location:**
   Where it is stored:
   Storage is held on Amazon Web Services (AWS) on their EU-West London.
   Data movement:
   The data only leaves these servers to be treated by third party applications (OpenAI, Anthropic) that anonymise the data before usage. Automwrite acts as a Data Processor, OpenAI and Anthropic are data sub-processors. Both OpenAI and Anthropic are GDPR and Data Protection compliant, please see their policies here:

   - OpenAI: https://openai.com/enterprise-privacy/
   - Anthropic: https://privacy.anthropic.com/en/collections/10663361-commercial-customers

2. **Security Measures**
   How we protect your data
   Encryption type: All data in transit is encrypted using HTTPS encryption (also referred to as SSL or TLS). Passwords are hashed using the BCrypt2 hashing algorithm and are never stored in plaintext.
   Access controls: All users must authenticate before accessing any data. The system employs role-based access controls to ensure that only appropriately assigned individuals can access relevant features, views, and data. Authorization to data sets is performed by validating the user's permissions against the attributes associated with each data set.
   Security certifications: Our cloud infrastructure providers' (AWS) physical and environmental security controls are audited for **SOC 2 Type II** and **ISO 27001** compliance.

   Monitoring
   How we monitor for breaches: We have documented internal procedures for ongoing monitoring of systems for both availability and resilience.
   How we notify clients of issues: In the event of an incident, we have procedures in place for customer notification using systems outside our standard network infrastructure, ensuring notifications can be sent even if main systems are unavailable. We would be in direct contact with our clients in the event of any issue.
   Response time commitments: Our target incident response time is **72 hours**.

3. **Data Control**

   Ownership
   Who owns the data: We act as data processors on your behalf, your data is used to the extent our software requires it in order to provide you with your letters and to improve our product.
   Who can access it: Access is restricted to authorized personnel who require it to perform their duties. Customers control who has access to their data within the application.
   How access is controlled: Access is controlled through role-based access controls, authentication mechanisms, and permissions assigned within the system. All users must authenticate before accessing any data.

   Data protection: Automwrite is registered with the Information Commissioner's Office (ICO), the UK's data protection regulator as "Automwrite Ltd" number ZB751705

47 Southgate St.
Winchester
SO23 9EH

www.automwrite.co.uk

Logan.Gibson@automwrite.co.uk
Wesley.Gibson@automwrite.co.uk

4. Access Management

How to request access: Access requests can be made through our support channels or directly to our technical support team at **liam.read@automwrite.co.uk**.
How to remove access: Access can be removed by the customer's administrator or by submitting a request to our support team via the above email.
Audit trail availability: All key changes by users, including changes to settings, user account creation and deletion, and user role changes, are logged in the system. Audit logs are available upon request or within the system for the customer's site administrator.

5. Data Deletion

During Service
How to delete data: Customers have the ability to delete any personal data at any time through the application interface, go into settings and you are able to delete your account. This deletes all of the user's data provided it is not associated with the organization. The root user can delete an organization with all of the associated data.
Time to complete deletion: Deletion requests are processed immediately when performed through the application.
Deletion confirmation process: Upon deletion, confirmation is provided within the application interface.

After Service Ends
What happens to your data: After termination of service, your data will be deleted after **30 days**.

How to export data
You can request a data export by contacting: **logan.gibson@automwrite.co.uk**.
Timeline for removal: Data will be permanently removed within **7 days** upon request.

6. Support Information

Key Contacts

- Technical support: daniel.braghis@autowrite.co.uk
- Compliance: logan.gibson@automwrite.co.uk

Emergency Response

- 24/7 contact: logan.gibson@automwrite.co.uk
- Incident response time: 8h