Cowrite GDPR Compliance

Description of the Processing

Cowrite stores and manages personal data linked to users' application documents, including contact information, CV and personal letters. Cowrite is the controller of our users' data. When a new account is created, users consent to the processing of their personal data by actively ticking a box with a corresponding link to Cowrite's Terms and Conditions, which also contains Cowrite's Privacy Policy.

Categories of Personal Data Processed

Subject to the user's input, processing of the following categories may be permissible:

1. Contact information: name, phone number, address, email address, and social media accounts.
2. Profile picture
3. Education and qualifications: academic qualifications, certifications, and awards.
4. Work experience: past and current employers, job titles, dates of employment and job descriptions.
5. Skills: technical, language, and leadership skills.
6. Interests and hobbies: any extra-curricular activities, such as sports, volunteering, or hobbies.
7. References: contact information of professional references.

Nature of the Processing

Cowrite stores personal data about users so that they can create and modify their application documents (CV and cover letter).

Duration of the Processing

The personal data is stored as long as the user has an active account. If an account has not been used for 6 months, it is considered inactive. If the user chooses to delete the data, it is stored in our backups for 30 + 30 days.

Processing by (Sub-) Processors

1. Urafiki AB, located within the EU, in its role of maintaining and developing the Cowrite Platform.
2. Google Cloud Platform / Firebase (Google Ireland Limited), located within the EU (eur3 region: Belgium/Netherlands), in its role of cloud infrastructure, database (Firestore), user authentication (Firebase Auth), file storage (Firebase Storage), serverless compute (Cloud Functions), and usage analytics (Firebase Analytics).
3. Google Gemini, located within the EU, in its role of AI Engine supplier.

Technical and Organisational Measures to Ensure the Security of the Data

- **Data storage location:** The data is stored in Google Cloud's eur3 multi-region (Belgium and Netherlands), within the EU. Google is responsible for physical protection of personal data at its data centers, which are certified under ISO 27001, SOC 2, and SOC 3.

- Application environment: Secure operating environment provided by Google Cloud Platform, including firewalls, DDoS protection, VPC network isolation, redundant power supply, and encryption (AES-256 standard for stored data, managed via Google Cloud KMS).

- Data transmission: All communication is encrypted using TLS 1.2 or higher.
- User authentication: User authentication is managed through Firebase Authentication. Passwords are hashed using industry-standard algorithms (bcrypt/scrypt). Cowrite supports Single Sign-On (SSO) via OpenID Connect and social login providers.

Measures for Data Minimisation

Cowrite strives to minimise data collection by only collecting the information essential for the users to create relevant application documents.

Measures for Limited Data Retention

The users' data is retained for a period set by the privacy policies for which they have given approval and is subsequently deleted. Deleted system users can no longer log in to the system.

Data Portability and Erasure

Users can export their data in a structured, commonly used, and machine-readable format. Upon request, user data is permanently erased from Cowrite's systems, including all backups, within a maximum of 60 days. Users can easily request removal from the system at any time by mailing Cowrite's support (support@cowrite.com). Personal data is also deleted after an account has been inactive for six months. Users are notified two weeks prior to the deletion.

Additional Measures

1. Data Processing Agreement (DPA): Cowrite and its subcontractors have signed separate DPAs specifying both parties' responsibilities under GDPR, including requirements for data security, user rights, and incident reporting. For Google Cloud Platform / Firebase, Cowrite has accepted the Google Cloud Data Processing Addendum, which governs Google's processing of personal data on Cowrite's behalf.

2. Privacy by Design: Cowrite applies the principle of Privacy by Design throughout the application's development lifecycle. This includes data minimisation, anonymisation where possible, and regular reviews of implemented security measures.

3. Rights for Registered Persons: Cowrite provides simple and clear mechanisms for users to exercise their GDPR rights, including access, rectification, erasure, and data portability. Requests are processed within 30 days at no additional cost to the user.

4. Risk Assessments: Cowrite conducts and documents Data Protection Impact Assessments (DPIA) for all data processing activities that are likely to result in high risks to individuals' rights and freedoms. Documentation is available upon request.

5. International Data Transfers: Cowrite's primary data storage is within the EU (Google Cloud eur3 region). Some Google sub-processors may be located in the United States; such transfers are covered by the EU-US Data Privacy Framework and Google's Standard Contractual Clauses (SCCs). For AI providers, Cowrite ensures all data transfers outside the EU/EEA are compliant with GDPR using SCCs or equivalent mechanisms. A list of Google's sub-processors is publicly available at cloud.google.com/terms/subprocessors.

Incident Handling

- **Immediate Reporting:** Any discovered incident involving data loss, corruption, or unauthorised access is reported immediately to Cowrite's Data Protection Officer (DPO).
- **Investigation:** The DPO conducts a prompt investigation to assess the extent and cause of the incident, identifying affected data and users.
- **Mitigation Measures:** Necessary steps are taken to limit damage, such as disabling affected accounts, notifying impacted users, and implementing technical measures to prevent recurrence.
- **Notification to Authorities:** Incidents posing a risk to individuals' rights and freedoms are reported to the relevant authority (e.g., Datainspektionen) within 72 hours.
- **User Notification:** If a high risk to users is identified, they are informed promptly with details of the incident, potential consequences, and measures taken.
- **Post-Incident Review:** Security policies are reviewed and updated, and staff training is enhanced as needed.

Firebase-Specific Data Processing

- **Firebase Analytics:** Usage analytics data is only collected after the user has given explicit consent via a cookie/consent banner implementing Google Consent Mode v2. Analytics data retention is set to a maximum of 14 months, after which it is automatically deleted.
- **Firebase Authentication:** Firebase Auth stores user email addresses, phone numbers (if provided), and authentication tokens. This data is stored in the EU and can be deleted programmatically via the Firebase Admin SDK upon user request.
- **Cloud Functions:** Serverless functions process data transiently in the eur3 region. No personal data is stored persistently by Cloud Functions beyond the processing required to fulfill the request.
- **Firebase Storage:** User-uploaded files (such as profile pictures) are stored in Firebase Storage in the eur3 region, encrypted at rest with AES-256 using Google-managed encryption keys.

Google Cloud Sub-Processor Transparency

Google maintains a publicly available list of sub-processors at cloud.google.com/terms/subprocessors. Cowrite monitors this list for changes and will notify affected customers of any material changes to sub-processors that may impact the processing of personal data. Customers may subscribe to notifications of sub-processor changes through Cowrite's support channels.

Document updated March 2026 to reflect migration from GleSYS/Microsoft Azure to Google Cloud Platform (Firebase).