Technical and Organizational Measures for Cloudsquid

Last update: October 2025

This document describes the requirements and implementation of measures for secure and compliant processing of personal data.

---

1. Confidentiality

1.1 Entry Control

Measures for preventing unauthorized individuals from accessing the premises where personal data are processed.

- Locked Building
- Electronic security locking system
- Mechanical security locking system
- Documented key issuance
- **Google Cloud-Infrastructure:** Our primary data processing and storage occurs on the infrastructure managed by Google Cloud in Frankfurt, Germany. These locations offer comprehensive physical security measures provided by Google.
- **Data flow to Azure:** Data requested by the user additionally flows to our Microsoft Azure account in Sweden to be processed in OpenAI models. Here, physical security is guaranteed by Microsoft's strict security measures.

1.2 Access Control

Measures for preventing unauthorized individuals from accessing the personal data processed digitally.

- Personalized User Accounts

- Complex Passwords
- Central Authentication
- Systems access is logged and monitored
- Secure line connection for external access (VPN)
- Use of an up-to-date firewall
- Multifactor access control
- **OAuth2 Authentication:** We use Firebase in combination with the OAuth2 protocol to authenticate users via Google. This allows for secure and reliable user login without us having to store passwords directly. Users are authenticated through their Google accounts, adding a strong layer of security.
- **Token-based Authorization:** After successful authentication by Google, a token is created that is used to authorize user actions within our application. This token ensures that only verified and authorized users have access to the corresponding data and functions.

1.3 Usage Control

Measures for restricting and monitoring accesses to personal data.

- Role-based authorization process
- Authentication with unique username and password
- Logging user access and processing
- Protected access to data storage media
- Encryption of data at rest
- Minimization of Superuser access
- **Customer Data Isolation:** Each customer has their own data stored in a separate PostgreSQL database, ensuring isolation of data between customers. Within a customer's organization, users have access to all of their company's data.

- **Continuous Monitoring:** Access is continuously monitored to detect unauthorized activity.
- **Data Encryption at Rest (Cloud Provider):** By default, data in Google Cloud is encrypted by the cloud provider using AES-256.
- **Internal Network Connectivity:** Databases and other critical services are only connected internally via the Cloud Virtual Private Cloud (VPC) network and are not directly accessible via the Internet.

1.4 Personal Data Minimization

Measures to minimize the use of personal data:

- Processing of personal data restricted to the minimal required for the defined purpose.
- Pseudonymization of personal data whenever feasible.
- **Specific Pseudonymization Measures:** Personal data is pseudonymized, where possible, using tokens or identifiers that separate data from direct identifiers (e.g., name, email).
- **Regular Data Review and Deletion:** Stored data is checked regularly and unnecessary data is deleted.
- **Anonymization:** Where possible, personal data is anonymized to reduce the amount of sensitive data stored.

1.5 Separation Control

Measures for separating personal data by means of various storage locations or logical separation:

- Separation of productive and test systems.
- Separation of personal data processing and storage and business logic systems.
- **Customer Data Isolation:** Each customer has their own data stored in a separate PostgreSQL database, ensuring isolation of data between customers.

---

2. Integrity

2.1 Transmission Control

Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorized persons during transmission:

- Data in transit required TLS (1.3).
- The use of private data storage media is prohibited.
- Connections to the infrastructure by employees are encrypted end-to-end.
- **Encryption and SSL Certificates:** We use SHA-1 for encryption and SSL certificates managed by Google Cloud to protect data in transit. The specific TLS version is used according to the standards implemented by Google Cloud (TLS version 1.0 or higher).
- **Data Integrity (Passwords/Tokens):** Data integrity for authentication is ensured by storing passwords and tokens when necessary using SHA-1 hash functions. A majority of the authentication processes are done via OAuth, which means we don't have to process passwords directly.

---

3. Availability and Reliability

Measures for protecting personal data against accidental destruction or loss:

- Regular documented patch management for servers.
- Physically separate redundant data storage or backup data.
- Regular documented patch management for endpoint devices.
- Uninterrupted power supply.
- Mitigate and remediate any confirmed zero-day vulnerabilities.
- Early fire detection in office buildings.
- Recovery procedures are established and tested at least annually.
- **Cloud Run Infrastructure for High Availability:** Our infrastructure is deployed as a Google Cloud Run module, meaning failover systems and high availability are managed directly by the Google Cloud Platform. This ensures that our services are always available and automatically restored in the event of any outages.

- **System Resilience (Google Cloud):** The resilience of our systems is ensured through the use of Google Cloud infrastructure, which supports regular testing and automatic scaling to meet demands and unexpected events.
- **Backup and Restore:** Automatic daily backups of all customer databases are created and stored securely in various geographically distributed locations within Google Cloud. These backups make it possible to quickly restore data in the event of a failure or data loss.
- **Redundancy and Failover (Google Cloud):** The Google Cloud Platform offers built-in redundancy mechanisms and failover systems that ensure that if individual components or regions fail, a backup infrastructure is automatically switched over, thereby minimizing downtime.
- **Regular Recovery Testing:** The recovery processes are tested regularly to ensure that data can be recovered quickly and effectively in the event of an emergency. The integrity and completeness of the secured data are also checked.

---

4. System Configuration and Monitoring

4.1 System Configuration

- Systems are set up according to the best security guidelines and the standard configurations of the respective cloud services.
- System configurations are regularly checked and updated.
- Changes to the system configuration are only possible by authorized persons.

4.2 Event Logging

- **Logging System:** Events are logged using Google Cloud's standard logging system.
- **Centralized Storage:** Log data is stored and managed centrally.
- **Access Controls:** Access to log data is restricted to authorized persons.
- **Security Event Detection:** Regular logging and monitoring are in place to ensure that security-related events are detected and handled appropriately.

---

5. Organizational Measures and Governance

5.1 Internal Governance and IT Security Management

- The CTO is responsible for IT governance and IT security.
- **ISO 27001 Certification:** We are ISO27001:2022 certified

5.2 Data Quality

- Incoming data is validated for accuracy and completeness when it is recorded.
- Users are allowed to update their data themselves or make corrections.

5.3 Data Retention

- **Data Retention Policies:** Clear data retention policies are implemented to ensure that personal data is only retained for as long as necessary to fulfill contractual obligations or legal requirements.
- **Automated Deletion:** After retention periods have expired, data will be securely deleted or anonymized, using automated processes where possible.
- **Regular Review:** Regular reviews of data holdings are carried out to ensure that no unnecessary or outdated personal data is retained.
- **User Control:** In certain cases, users are given control over their own data by offering them the opportunity to delete their data themselves or request deletion.

5.4 Accountability

- **Responsibilities:** The CPO is responsible for compliance with data protection regulations.
- **Internal Reviews:** Regular internal reviews are carried out.
- **Certification:** Cloudsquid is ISO27001:2022 certified. The report can be requested via the contact email.

5.5 Data Portability and Deletion

- **Data Export:** Tools are provided that allow users to export their data in a common, machine-readable format.
- **Deletion Processes:** Clearly defined processes are implemented for the secure deletion of personal data upon request or after contract termination.
- **Automated Deletion:** Automated mechanisms are used to delete data in accordance with the specified retention periods.

---

6. Processor and Sub-processor Measures

When transferring data to (sub)processors, the specific technical and organizational measures that the (sub)processor must take to support the controller are as follows:

- **Google Cloud Platform:** Google Cloud provides extensive documentation and assurances regarding their technical and organizational measures, including certifications like ISO 27001, SOC 1/2/3, and GDPR compliance, which support Cloudsquid's role as a controller.
- **Microsoft Azure/OpenAI:** Microsoft Azure and OpenAI also provide detailed security and compliance documentation, including certifications and adherence to relevant data protection standards, ensuring that data processed in their environments (e.g., for AI models) is protected with an adequate level of security.
- Cloudsquid ensures that appropriate Data Processing Agreements (DPAs) are in place with all sub-processors, obligating them to implement security measures consistent with Cloudsquid's own standards and applicable data protection laws.
- Regular due diligence is conducted on sub-processors to verify their ongoing compliance and security posture.