EQS GROUP

Technical and Organizational Measures for EQS Cloud Services

according to Art. 32 EU GDPR

TOMs_EQS Cloud Services_en - Status 30/10/2024

Foreword

This document covers the technical and organizational security measures (TOMs) taken by EQS Group within the meaning of Art. 32 EU GDPR resulting from the data processing described in the underlying Agreement. The following TOM apply generally to all Cloud Services of EQS Group.

Organizations which collect, process or use personal data themselves or on their behalf must take appropriate technical and organizational security measures to ensure an adequate level of protection.

EQS Group meets this requirement through the following measures.

Content:

1. General

Data Protection Officer:	Oliver Kunert, External DPO Sunny Systems GmbH
Contact details:	dataprotection@eqs.com
Formally appointed on:	15.12.2015
Position in the company:	Reports directly to the Executive Board

At regular intervals – at least once a year – internal audits or supplements to the existing audit are carried out and all technical and organizational security measures are checked and updated if necessary.

All employees are instructed in the requirements of data protection when they are hired. Every employee receives training on data protection, either in person by the data protection officer or via an online tool.

EQS Group has implemented an information security management system and is certified according to ISO 27001.

Please note that recent acquisitions may not implement all of the below controls and are currently not part of our information security management system. However, EQS Group is working towards implementing these controls and including recent acquisitions into the certification scope in due course.

Furthermore, cutting edge technologies, like functionality that involves "Generative AI", may not implement all of the below controls, as limitations at our Suppliers apply.

2. Confidentiality

according to Art. 32 para. 1 lit. b EU GDPR

a) Physical access control

The following measures have been implemented to restrict or prevent unauthorized access to premises where personal data is processed.

› Highly secure and ISO 27001 certified data centres
› Alarm system and/or security service
› Security locks
› Key Management
› Access only for authorized employees
› Definition of security zones with highly restricted access rights ("Needs-Access" principle)
› Automated physical access control systems (e.g., chip cards or transponder systems)
› Visitor control (logging and escorting of visitors)
› No unescorted access for external persons to server rooms
› Mandatory corporate guidelines for all employees
› Careful selection of external personnel and service providers

b) Logical access control

The following measures have been implemented to prevent data processing facilities of EQS Group from being used by unauthorized persons.

› Anti-virus software on server and client
› Separation of administrative and user accounts
› Firewalls
› Password rules and policy (complexity, length and expiration)
› VPN for remote access
› "Clean Desk / Clear Screen Policy
› Automatic desktop lock
› Administration and regular review of user authorizations
› Encryption of (external) data carriers, smartphones and notebooks/tablets
› Allocation of authorizations according to the "need-to-know" principle
› Intrusion detection systems
› Guidelines on data protection and IT security

c) Data access control

The following measures have been implemented to ensure that personal data can only be accessed in accordance with the assigned authorizations. In addition, it is ensured that personal data cannot be processed without authorization, i.e. cannot be recorded, read, copied, changed or deleted without authorization.

› Authorization concept with differentiated authorization assignment
› Number of administrative users limited to a necessary minimum
› Logging of accesses to applications, specifically when entering, changing and deleting data
› Management of user rights by administrators
› User identification and authentication
› Authorization and access rules
› Encryption in motion and at rest
› Locking of sensitive personal data and confidential information
› File shredder according to DIN 66399 or external service provider for data destruction
› Written regulations for the handling of electronic operating devices

d) Separation control

The following measures have been implemented to ensure that data collected for different purposes are processed separately.

› Separation of productive and test environment
› Authorization concept for access to data
› Secure software configurations
› No processing of productive data in test environment
› Customer separation (at least logical separation)
› Customer data is only processed for the contractually defined purposes
› Encryption
› Separated networks

e) Anonymization / pseudonymization of personal data

Where necessary, the following measures are implemented to prevent personal data from being attributed to a specific data subject without the use of additional information.

› Personal data must be deleted or anonymized / pseudonymized after expiry of the statutory retention period if deletion is not possible.
› Functions for anonymization / pseudonymization of data
› No logging of IP address data or other metadata of whistle blowers
› Secure and, if desired, anonymous communication with whistle blowers

3. Integrity

according to Art. 32 para. 1 lit. b EU GDPR

a) Data transfer control

The following data integrity measures are implemented, which generally help to protect against unauthorized or unlawful processing, destruction or accidental damage.

› Encrypted connections for the transmission of data
› Documentation of the data recipients and the duration of the planned transfer or deletion periods
› Logging of the data transmission
› Use of VPN technology
› Key management and access management process
› Company policy
› Multi-factor authentication
› Processing of data outside the offices strictly regulated
› Security provisions for the storage of data media
› Destruction of data media by certified company
› Due diligence in the selection of transport companies
› Safe transport containers

b) Input control

The following measures have been implemented to ensure that it is possible to verify by whom personal data has been entered, modified or removed.

› Technical logging of the entry, modification and deletion of data
› Assignment of rights to enter, change and delete data based on an authorization concept
› Review of protocols
› Traceability of input, change, deletion through individual usernames
› Clear responsibilities for deletions
› Retention of forms from which data have been transferred to automated processing operations

4. Availability and resilience

according to Art. 32 para. 1 lit. b EU GDPR

a) Availability control

The following measures have been implemented to ensure that personal data is protected against destruction or loss:

› Fire and smoke detection systems
› Emergency and safety concept
› Fire extinguishers and air conditioning in server rooms
› Review of backup process
› Uninterruptible power supply
› Virus protection concept
› Monitoring of temperature and humidity in server rooms
› Redundancy of important system components
› Regular control and maintenance of all systems

b) Recoverability

The following measures are implemented to ensure that personal data can be recovered quickly:

› Redundant infrastructure
› Regular backups
› Regular and encrypted backups of customer data
› off-site backup storage
› Regular checking of backups for availability, completeness and integrity

5. Procedures for regular testing, assessment and evaluation

according to Art. 32 para. 1 lit. d DSGVO and Art. 25 para. 1 DSGVO

a) Data protection management

› Appointed data protection officer
› Security certifications according to ISO 27001
› Use of software solutions for data protection management
› Regular training of employees and commitment of all employees to confidentiality
› Privacy by default
› Data protection certifications for selected products of EQS Group
› Verification of the effectiveness of the technical security measures, e.g., by means of regular audits
› Company policy on data protection
› Central documentation of all procedures and regulations on data protection with access for employees according to need / authorization
› If required, implementation of data protection impact assessment according to Art. 35 EU GDPR
› Documented security concept
› Documented processes for handling data protection incidents as well as data subject requests

b) Incident response management

› Documented process for detecting and reporting security incidents / data breaches
› Intrusion detection system (IDS)
› Antivirus software
› Firewalls
› Documentation of security incidents and data breaches as part of the information security management system
› Formal process and responsibilities for follow-up of security incidents and data breaches

c) Information security management system

› Internal information security officer (CISO)
  E-mail address: infosec@eqs.com
› Security certifications according to ISO 27001
› Regular review of the effectiveness of the technical security measures
› Information security management system (ISMS)

d) Processor control

› Careful selection and monitoring of subcontractors, considering information security aspects
› Concluded data processing agreement
› Regular review of the execution of the contract
› Destruction of data after the end of the contract
› Regulated use of further subcontractors