Misure tecniche e organizzative per i Servizi Cloud di EQS

secondo l'art. 32 UE GDPR (versione bilingue italiano/inglese)

TOMs_EQS Cloud Services_it-en- Status 30/10/2024

Prefazione

Questo documento è stato preparato sia in italiano che in inglese. In caso di incongruenza, la versione inglese sarà applicabile e vincolante per le parti.

Il documento descrive le misure di sicurezza tecniche e organizzative ("TOM") adottate da EQS Group ai sensi dell'art. 32 del Regolamento Europeo 2016/679 ("UE GDPR") derivanti dal trattamento dei dati descritto nel Contratto sottostante. I seguenti TOM si applicano in generale a tutti i Servizi Cloud del EQS Group.

Le organizzazioni che raccolgono, elaborano o utilizzano dati personali in proprio o per loro conto devono adottare misure di sicurezza tecniche e organizzative appropriate per garantire un adeguato livello di protezione.

EQS Group soddisfa questo requisito attraverso le seguenti misure.

Foreword

This document has been prepared in both Italian and English. In the event of any inconsistency, the English version shall apply and be binding upon the parties.

The document describes 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 TOMs 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.

Contenuto

1. Generale

Responsabile della protezione dei dati:
Oliver Kunert, Responsabile per la protezione dei dati esterno, Sunny Systems GmbH
Dettagli di contatto:
dataprotection@eqs.com
Formalmente nominato il: 15.12.2015
Posizione nell'azienda: Riferisce direttamente al Consiglio Direttivo

Ad intervalli regolari - almeno una volta all'anno - vengono eseguiti audit interni o integrazioni all'audit esistente e tutte le misure di sicurezza tecniche e organizzative vengono controllate e aggiornate se necessario.

Tutti i dipendenti vengono istruiti sui requisiti della protezione dei dati al momento dell'assunzione. Ogni dipendente riceve una formazione sulla protezione dei dati, di persona da parte del responsabile della protezione dei dati o tramite uno strumento online.

EQS Group ha implementato un sistema di gestione della sicurezza delle informazioni certificato secondo ISO 27001.

Si prega di notare che le recenti acquisizioni potrebbero non implementare tutti i controlli sottoelencati e che attualmente non sono incluse nel nostro sistema di gestione della sicurezza delle informazioni. Tuttavia, EQS sta lavorando per implementare questi controlli e includere le recenti acquisizioni nell'ambito della certificazione a tempo debito.

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 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",

Inoltre, le tecnologie all'avanguardia, come le funzionalità che coinvolgono l'"IA generativa", potrebbero non implementare tutti i controlli indicati di seguito, in quanto si applicano le limitazioni dei nostri fornitori.

may not implement all of the below controls, as limitations at our Suppliers apply.

2. Riservatezza

secondo l'art. 32 para. 1 capo b UE GDPR

a) Controllo dell'accesso fisico

Le seguenti misure sono state implementate per limitare o impedire l'accesso non autorizzato ai locali in cui vengono trattati i dati personali.

- Centri dati altamente sicuri e certificati ISO 27001
- Sistema di allarme e/o servizio di sicurezza
- Serrature di sicurezza
- Gestione delle chiavi
- Accesso solo per i dipendenti autorizzati
- Definizione di zone di sicurezza con diritti di accesso molto limitati (principio "Needs-Access")
- Sistemi automatizzati di controllo dell'accesso fisico (per esempio, carte con chip o sistemi a transponder)
- Controllo dei visitatori (registrazione e accompagnamento dei visitatori)
- Nessun accesso senza scorta di persone esterne alle stanze dei server
- Linee guida aziendali obbligatorie per tutti i dipendenti
- Attenta selezione del personale esterno e dei fornitori di servizi

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) Controllo dell'accesso logico

Le seguenti misure sono state implementate per evitare che le strutture di elaborazione dati di EQS Group vengano utilizzate da persone non autorizzate.

- Software antivirus su server e client
- Separazione degli account amministrativi e degli utenti
- Firewall
- Regole e politica delle password (complessità, lunghezza e scadenza)
- VPN per l'accesso remoto
- Politica della scrivania pulita / schermo sgombro
- Blocco automatico del desktop
- Amministrazione e revisione regolare delle autorizzazioni degli utenti
- Crittografia di supporti dati (esterni), smartphone e notebook/tablet
- Assegnazione delle autorizzazioni secondo il principio del "need-to-know"
- Sistemi di rilevamento delle intrusioni
- Linee guida sulla protezione dei dati e sulla sicurezza informatica

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) Controllo dell'accesso ai dati

Le seguenti misure sono state implementate per garantire che i dati personali possano essere accessibili solo in conformità con le autorizzazioni assegnate. Inoltre, EQS garantisce che i dati personali non possano essere elaborati senza autorizzazione, ovvero non possano essere registrati, letti, copiati, modificati o cancellati senza autorizzazione.

- Concetto di autorizzazione con assegnazione di autorizzazione differenziata
- Numero di utenti amministrativi limitato al minimo necessario
- Registrazione degli accessi alle applicazioni, in particolare durante l'inserimento, la modifica e la cancellazione dei dati
- Gestione dei diritti degli utenti da parte degli amministratori
- Identificazione e autenticazione dell'utente
- Regole di autorizzazione e di accesso
- Crittografia in movimento e a riposo
- Blocco dei dati personali sensibili e delle informazioni riservate
- Tritacarte conforme a DIN 66399 o fornitore di servizi esterno per la distruzione dei dati
- Regole scritte per la manipolazione dei dispositivi operativi elettronici

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) Controllo della separazione

Le seguenti misure sono state implementate per garantire che i dati raccolti per scopi diversi siano trattati separatamente.

- Separazione dell'ambiente produttivo e di test
- Concetto di autorizzazione per l'accesso ai dati
- Configurazioni software sicure
- Nessuna elaborazione di dati produttivi in ambiente di test
- Separazione dei clienti (per lo meno logica)
- I dati dei clienti sono trattati solo per gli scopi definiti contrattualmente
- Crittografia
- Reti separate

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) Anonimizzazione / pseudonimizzazione dei dati personali

Dove necessario, sono adottate le seguenti misure per evitare che i dati personali vengano attribuiti a una specifica persona interessata senza l'uso di informazioni aggiuntive.

- I dati personali devono essere cancellati o resi anonimi / pseudonimizzati dopo la scadenza del periodo di conservazione legale, se la cancellazione non è possibile.
- Funzioni per l'anonimizzazione / pseudonimizzazione dei dati
- Nessuna registrazione dei dati degli indirizzi IP o di altri metadati degli informatori
- Comunicazione sicura e, se desiderato, anonima con gli informatori

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. Integrità

secondo l'art. 32 para. 1 capo b UE GDPR

a) Controllo del trasferimento dei dati

Vengono implementate le seguenti misure di integrità dei dati, che in generale aiutano a proteggere contro l'elaborazione non autorizzata o illegale, la distruzione o il danneggiamento accidentale.

- Connessioni criptate per la trasmissione di dati
- Documentazione dei destinatari dei dati e la durata dei periodi di trasferimento o di cancellazione
- Registrazione della trasmissione dei dati
- Uso della tecnologia VPN
- Processo di gestione delle chiavi e degli accessi
- Politica aziendale
- Autenticazione a più fattori
- Trattamento dei dati al di fuori degli uffici strettamente regolamentato
- Disposizioni di sicurezza per la conservazione dei supporti di dati
- Distruzione dei supporti di dati da parte di un'azienda certificata
- Due diligence nella selezione delle aziende di trasporto
- Contenitori per il trasporto sicuro

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) Controllo dell'input

Le seguenti misure sono state implementate per garantire che sia possibile verificare da chi sono stati inseriti, modificati o rimossi i dati personali.

- Registrazione tecnica dell'inserimento, della modifica e della cancellazione dei dati
- Assegnazione dei diritti per inserire, modificare e cancellare dati basati su un concetto di autorizzazione
- Revisione dei protocolli
- Tracciabilità dell'input, modifiche, cancellazioni attraverso nomi utente individuali
- Responsabilità chiaramente identificate per le cancellazioni
- Conservazione dei moduli da cui i dati sono stati trasferiti a trattamenti automatizzati

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. Disponibilità e resilienza

secondo l'art. 32 para. 1 capo b UE GDPR

a) Controllo della disponibilità

Le seguenti misure sono state implementate per garantire che i dati personali siano protetti dalla distruzione o dalla perdita:

- Sistemi di rilevamento del fuoco e del fumo
- Concetto di emergenza e sicurezza
- Estintori e aria condizionata nelle sale server
- Revisione del processo di backup
- Gruppo di continuità elettrico
- Concetto di protezione dai virus
- Monitoraggio della temperatura e dell'umidità nelle sale server
- Ridondanza di componenti importanti del sistema
- Controllo e manutenzione regolari di tutti i sistemi

b) Recuperabilità

Le seguenti misure sono attuate per garantire che i dati personali possano essere recuperati rapidamente:

- Infrastruttura ridondante
- Backup regolari
- Backup regolari e criptati dei dati dei clienti
- Archiviazione di backup off-site
- Controllo regolare dei backup per disponibilità, completezza e integrità

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. Procedure per test, valutazioni e accertamenti regolari

secondo l'art. 32 para. 1 capo d e l'art. 25 para. 1 UE GDPR

a) Gestione della protezione dei dati

- Nominato responsabile della protezione dei dati
- Certificazioni di sicurezza secondo ISO 27001
- Utilizzo di soluzioni software per la gestione della protezione dei dati
- Formazione regolare dei dipendenti e impegno di tutti i dipendenti alla riservatezza
- Privacy per impostazione predefinita
- Certificazioni di protezione dei dati per prodotti selezionati di EQS Group
- Verifica dell'efficacia delle misure tecniche di sicurezza, per esempio, per mezzo di audit regolari
- Politica aziendale sulla protezione dei dati
- Documentazione centrale di tutte le procedure e i regolamenti sulla protezione dei dati con accesso per i dipendenti in base alla necessità / autorizzazione
- Se necessario, attuazione della valutazione d'impatto sulla protezione dei dati secondo l'art. 35 UE GDPR
- Concetto di sicurezza documentato
- Processi documentati per gestire gli incidenti relativi alla protezione dei dati e le richieste degli interessati

5. Procedures for regular testing, assessment and evaluation

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

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) Gestione della risposta agli incidenti

- Processo documentato per rilevare e segnalare incidenti di sicurezza / violazioni di dati
- Sistema di rilevamento delle intrusioni (IDS)
- Software antivirus
- Firewall
- Documentazione degli incidenti di sicurezza e delle violazioni dei dati come parte del sistema di gestione della sicurezza delle informazioni
- Processo formale e responsabilità per il follow-up degli incidenti di sicurezza e delle violazioni dei dati

c) Sistema di gestione della sicurezza delle informazioni

- Responsabile interno della sicurezza delle informazioni (CISO)
  Indirizzo e-mail: infosec@eqs.com
- Certificazioni di sicurezza secondo ISO 27001
- Revisione regolare dell'efficacia delle misure tecniche di sicurezza
- Sistema di gestione della sicurezza delle informazioni (ISMS)

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) Controllo del processore

- Attenta selezione e monitoraggio dei subappaltatori, considerando gli aspetti della sicurezza delle informazioni
- Accordo concluso per il trattamento dei dati
- Revisione regolare dell'esecuzione del contratto
- Distruzione dei dati dopo la fine del contratto
- Uso regolamentato dei subappaltatori

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