» Mesures techniques et organisationnelles pour EQS Cloud Services «

conformément à l'art. 32 du RGPD de L'UE (version bilingue français /anglais)

TOMs_EQS Cloud Services_fr-en- Status 10/12/2021 12:18:00

Avant-propos

Ce document a été préparé en français et en anglais. En cas d'incohérence,veuillez vous référer à la version anglaise.

Le document décrit les mesures de sécurité techniques et organisationnelles ('TOMs') prises par EQS Group au sens de l'art. 32 RGPD de l'UE résultant du traitement des données décrit dans l'accord sous-jacent. Les 'TOMs' suivantes s'appliquent de manière générale à toutes les 'Cloud Services' d'EQS Group.

Les organisations qui collectent, traitent ou utilisent des données à caractère personnel, elles-mêmes ou en leur nom, doivent prendre des mesures de sécurité techniques et organisationnelles appropriées afin de garantir un niveau de protection adéquat.

EQS Group répond à cette exigence par les mesures suivantes.

Foreword

This document has been prepared in both French 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.

Contenu

1. Général

Délégué à la protection des données :
Oliver Kunert,
DPD externe, Sunny Systems GmbH
Coordonnées de contact :
dataprotection@eqs.com
Officiellement nommé le : 15.12.2015
Position dans l'entreprise : Rapporte directement au Conseil d'administration

À intervalles réguliers - au moins une fois par an - des audits internes ou des compléments à l'audit existant sont effectués et toutes les mesures de sécurité techniques et organisationnelles sont vérifiées et mises à jour si nécessaire.

Tous les employés sont instruits des exigences de la protection des données lors de leur embauche. Chaque employé reçoit une formation sur la protection des données, soit en personne par le délégué à la protection des données, soit via une formation en ligne.

EQS Group AG a mis en place un système de gestion de la sécurité de l'information et est certifié selon la norme ISO 27001.

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

2. Confidentialité

conformément à l'art. 32 para. 1 lit. b RGDP

a) Contrôle d'accès physique

Les mesures suivantes ont été mises en œuvre pour restreindre ou empêcher l'accès non autorisé aux locaux où les données personnelles sont traitées.

- Centres de données hautement sécurisés et certifiés ISO 27001
- Système d'alarme et/ou service de sécurité
- Serrures de sécurité
- Gestion des clés
- Accès uniquement pour les employés autorisés
- Définition de zones de sécurité avec des droits d'accès très restreints (principe "Besoins-Accès")
- Systèmes automatisés de contrôle d'accès physique (par exemple, cartes à puce ou systèmes de transpondeurs)
- Contrôle des visiteurs (enregistrement et escorte des visiteurs)
- Pas d'accès sans escorte aux salles de serveurs pour les personnes extérieures.
- Directives d'entreprise obligatoires pour tous les employés
- Sélection minutieuse du personnel et des prestataires de services externes

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) Contrôle d'accès logique

Les mesures suivantes ont été mises en œuvre pour empêcher l'utilisation des installations de traitement des données d'EQS Group par des personnes non autorisées.

- Logiciel anti-virus sur le serveur et le client
- Séparation des comptes administratifs et des comptes utilisateurs
- Pare-feu
- Règles et politique en matière de mots de passe (complexité, longueur et expiration)
- VPN pour l'accès à distance
- Politique du bureau propre et de l'écran vide
- Verrouillage automatique du bureau
- Administration et révision régulière des autorisations des utilisateurs
- Chiffrement des supports de données (externes), des smartphones et des ordinateurs portables/tablettes.
- Attribution des autorisations selon le principe du "besoin d'en connaître".
- Systèmes de détection d'intrusion
- Lignes directrices sur la protection des données et la sécurité informatique

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) Contrôle d'accès aux données

Les mesures suivantes ont été mises en œuvre pour garantir que les données personnelles ne peuvent être consultées que conformément aux autorisations attribuées. En outre, il est garanti que les données personnelles ne peuvent être traitées sans autorisation, c'est-à-dire qu'elles ne peuvent être enregistrées, lues, copiées, modifiées ou supprimées sans autorisation.

- Concept d'autorisation avec affectation différenciée des autorisations
- Nombre d'utilisateurs administratifs limité à un minimum nécessaire
- Enregistrement des accès aux applications, notamment lors de la saisie, de la modification et de la suppression de données.
- Gestion des droits des utilisateurs par les administrateurs
- Identification et authentification des utilisateurs
- Règles d'autorisation et d'accès
- Le chiffrement en mouvement et au repos
- Verrouillage des données personnelles sensibles et des informations confidentielles
- Broyeur de fichiers selon la norme DIN 66399 ou prestataire de services externe pour la destruction de données
- Réglementation écrite pour la manipulation des dispositifs d'exploitation électroniques

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) Contrôle de la séparation

Les mesures suivantes ont été mises en œuvre pour garantir que les données collectées à des fins différentes sont traitées séparément.

- Séparation de l'environnement de production et de test
- Concept d'autorisation pour l'accès aux données
- Configurations logicielles sécurisées
- Pas de traitement des données productives dans l'environnement de test
- Séparation des clients (au moins une séparation logique)
- Les données des clients ne sont traitées qu'aux fins définies contractuellement.
- Cryptage
- Réseaux séparés

e) Anonymisation / pseudonymisation des données personnelles

Le cas échéant, les mesures suivantes sont mises en œuvre pour empêcher que des données personnelles soient attribuées à une personne concernée spécifique sans l'utilisation d'informations supplémentaires.

- Les données personnelles doivent être supprimées ou rendues anonymes / pseudonymes après l'expiration de la période de conservation légale si la suppression n'est pas possible.
- Fonctions d'anonymisation / pseudonymisation des données
- Pas d'enregistrement des adresses IP ou autres métadonnées des lanceurs d'alerte.
- Communication sécurisée et, si désiré, anonyme avec les lanceurs d'alerte.

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. Intégrité

conformément à l'art. 32 para. 1 lit. b RGDP

a) Contrôle du transfert de données

Les mesures d'intégrité des données suivantes sont mises en œuvre, qui contribuent généralement à la protection contre le traitement non autorisé ou illégal, la destruction ou les dommages accidentels.

- Connexions cryptées pour la transmission de données
- Documentation des destinataires des données et de la durée des périodes de transfert ou de suppression prévues.
- Enregistrement de la transmission des données
- Utilisation de la technologie VPN
- Processus de gestion des clés et des accès
- Politique de l'entreprise
- Authentification multi-facteurs
- Le traitement des données en dehors des bureaux est strictement réglementé
- Dispositions de sécurité pour le stockage des supports de données
- Destruction des supports de données par une entreprise certifiée
- Diligence raisonnable dans la sélection des entreprises de transport
- Des conteneurs de transport sûrs

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) Contrôle des entrées

Les mesures suivantes ont été mises en œuvre pour garantir un processus de vérification pour la personne qui a introduit, modifié ou supprimé des données personnelles.

- Enregistrement technique de l'entrée, de la modification et de la suppression des données.
- Attribution des droits d'entrée, de modification et de suppression des données sur la base d'un concept d'autorisation.
- Révision des protocoles
- Traçabilité de l'entrée, de la modification et de la suppression par le biais de noms d'utilisateur individuels.
- Des responsabilités claires pour les suppressions
- Conservation des formulaires à partir desquels les données ont été transférées vers des traitements automatisés

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. Disponibilité et résilience

conformément à l'art. 32 para. 1 lit. b RGDP

a) Contrôle des disponibilités

Les mesures suivantes ont été mises en œuvre pour garantir que les données personnelles sont protégées contre la destruction ou la perte :

- Systèmes de détection d'incendie et de fumée
- Concept d'urgence et de sécurité
- Extincteurs et climatisation dans les salles de serveurs
- Examen du processus de sauvegarde
- Alimentation électrique ininterrompue
- Concept de protection contre les virus
- Surveillance de la température et de l'humidité dans les salles de serveurs
- Redondance des composants importants du système
- Contrôle et entretien réguliers de tous les systèmes

b) Récupérabilité

Les mesures suivantes sont mises en œuvre pour garantir une récupération rapide des données personnelles :

- Infrastructure redondante
- Sauvegardes régulières
- Sauvegardes régulières et cryptées des données des clients
- Stockage de sauvegarde hors site
- Vérification régulière de la disponibilité, de l'exhaustivité et de l'intégrité des sauvegardes.

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. Procédures d'examen, d'évaluation et de contrôle réguliers

conformément à l'art. 32 para. 1 lit. d et l'art. 25 para. 1 RGPD

a) Gestion de la protection des données

- Désignation d'un délégué à la protection des données
- Certifications de sécurité selon la norme ISO 27001
- Utilisation de solutions logicielles pour la gestion de la protection des données
- Formation régulière des employés et engagement de tous les employés à la confidentialité
- La confidentialité par défaut
- Certifications de protection des données pour certains produits d'EQS Group
- Vérification de l'efficacité des mesures techniques de sécurité, par exemple au moyen d'audits réguliers.
- Politique de l'entreprise en matière de protection des données
- Documentation centrale de toutes les procédures et réglementations sur la protection des données avec accès pour les employés en fonction des besoins/autorisations.
- Si nécessaire, mise en œuvre d'une analyse d'impact sur la protection des données conformément à l'art. 35 du RGPD de l'UE

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) Gestion de la réponse aux incidents

- Processus documenté pour détecter et signaler les incidents de sécurité / les violations de données
- Système de détection d'intrusion (IDS)
- Logiciel antivirus
- Pare-feu
- Documentation des incidents de sécurité et des violations de données dans le cadre du système de gestion de la sécurité de l'information.
- Processus et responsabilités formels pour le suivi des incidents de sécurité et des violations de données

c) Système de gestion de la sécurité de l'information

- Responsable de la sécurité informatique interne (CISO)
  Adresse électronique : infosec@eqs.com
- Certifications de sécurité selon la norme ISO 27001
- Examen régulier de l'efficacité des mesures techniques de sécurité
- Système de management de la sécurité de l'information (SMSI)

d) Contrôle du processeur

- Sélection et contrôle minutieux des sous-traitants, en tenant compte des aspects liés à la sécurité des informations.
- Accord conclu sur le traitement des données
- Examen régulier de l'exécution du contrat
- Destruction des données après la fin du contrat
- Recours réglementé à d'autres sous-traitants

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