» Srodki techniczne i organizacyjne dla Usług w Chmurze EQS Group «

zgodnie z Art. 32 EU GDPR (wersja dwujęzyczna polski / angielski)

TOMs_EQS Cloud Services_pl-en- Status 10/12/2021 12:19:00

Przedmowa

Niniejszy dokument został sporządzony zarówno w języku polskim jak i angielskim. W przypadku jakichkolwiek rozbieżności, wersja angielska będzie obowiązywać i będzie wiążąca dla stron.

Niniejszy dokument opisuje techniczne i organizacyjne środki bezpieczeństwa ("TOM") podjęte przez EQS Group w rozumieniu Art. 32 EU GDPR wynikające z przetwarzania danych opisanego w Umowie bazowej. Poniższe TOM-y mają ogólne zastosowanie do wszystkich Usług w Chmurze EQS Group.

Organizacje, które gromadzą, przetwarzają lub wykorzystują dane osobowe samodzielnie lub w swoim imieniu, muszą podjąć odpowiednie techniczne i organizacyjne środki bezpieczeństwa w celu zapewnienia odpowiedniego poziomu ochrony.

EQS Group spełnia ten wymóg poprzez następujące działania

Foreword

This document has been prepared in both Polish 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.

Treść

1. Ogólne

Inspektor ochrony danych:
Oliver Kunert,
zewnętrzny IOD Sunny Systems GmbH
Dane kontaktowe:
dataprotection@eqs.com
Formalnie powołany w dniu: 15.12.2015
Stanowisko w firmie: Podlega bezpośrednio Zarządowi

W regularnych odstępach czasu - co najmniej raz w roku - przeprowadzane są audyty wewnętrzne lub uzupełnienia istniejących audytów, a wszystkie techniczne i organizacyjne środki bezpieczeństwa są sprawdzane i w razie potrzeby aktualizowane.

Wszyscy pracownicy są instruowani w zakresie wymogów ochrony danych w momencie zatrudnienia. Każdy pracownik jest szkolony w zakresie ochrony danych osobiście przez inspektora ochrony danych lub za pomocą narzędzia online.

EQS Group AG wdrożyła system zarządzania bezpieczeństwem informacji i posiada certyfikat 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. Poufność

zgodnie z Art. 32 par. 1 lit. b EU GDPR

a) Fizyczna kontrola dostępu

Wdrożono następujące środki w celu ograniczenia lub zapobieżenia nieupoważnionemu dostępowi do pomieszczeń, w których przetwarzane są dane osobowe.

- Wysoce bezpieczne centra danych z certyfikatem ISO 27001
- System alarmowy i/lub usługi bezpieczeństwa
- Zamki bezpieczeństwa
- Zarządzanie kluczami
- Dostęp tylko dla upoważnionych pracowników
- Określenie stref bezpieczeństwa z wysoce ograniczonymi prawami dostępu (zasada "Potrzeby - Dostęp")
- Zautomatyzowane systemy fizycznej kontroli dostępu (np. karty chipowe lub systemy transponderowe)
- Kontrola gości (rejestrowanie i eskortowanie gości)
- Zakaz wstępu do serwerowni dla osób z zewnątrz bez eskorty
- Obowiązkowe wytyczne korporacyjne dla wszystkich pracowników
- Staranny dobór personelu zewnętrznego i dostawców usług

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) Logiczna kontrola dostępu

W celu uniemożliwienia korzystania z urządzeń do przetwarzania danych EQS Group przez osoby nieuprawnione, wdrożono następujące środki.

- Oprogramowanie antywirusowe na serwerze i kliencie
- Oddzielenie kont administracyjnych od kont użytkowników
- Zapory sieciowe
- Zasady i polityka dotyczące haseł (złożoność, długość i wygaśnięcie)
- VPN dla zdalnego dostępu
- "Polityka czystego biurka / czystego ekranu
- Automatyczna blokada pulpitu
- Administracja i regularny przegląd uprawnień użytkowników
- Szyfrowanie (zewnętrznych) nośników danych, smartfonów i notebooków/tabletów
- Przydzielanie uprawnień zgodnie z zasadą "wiedzy koniecznej".
- Systemy wykrywania włamań
- Wytyczne dotyczące ochrony danych i bezpieczeństwa informatycznego

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) Kontrola dostępu do danych

W celu zapewnienia, że dostęp do danych osobowych jest możliwy tylko zgodnie z przypisanymi uprawnieniami, zastosowano następujące środki. Ponadto zapewniono, że dane osobowe nie mogą być przetwarzane bez upoważnienia, tzn. nie mogą być zapisywane, odczytywane, kopiowane, zmieniane lub usuwane bez upoważnienia.

- Koncepcja autoryzacji ze zróżnicowanym przydziałem uprawnień
- Liczba użytkowników administracyjnych ograniczona do niezbędnego minimum
- Rejestrowanie dostępu do aplikacji, w szczególności podczas wprowadzania, zmiany i usuwania danych
- Zarządzanie uprawnieniami użytkowników przez administratorów
- Identyfikacja i uwierzytelnianie użytkownika
- Zasady autoryzacji i dostępu
- Szyfrowanie w ruchu i w spoczynku
- Blokowanie wrażliwych danych osobowych i informacji poufnych
- Niszczarka do akt zgodnie z DIN 66399 lub zewnętrzny usługodawca w zakresie niszczenia danych
- Pisemne przepisy dotyczące obsługi elektronicznych urządzeń eksploatacyjnych

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) Kontrola separacji

W celu zapewnienia, że dane gromadzone w różnych celach są przetwarzane oddzielnie, zastosowano następujące środki.

- Rozdzielenie środowiska produkcyjnego i testowego
- Koncepcja autoryzacji dostępu do danych
- Bezpieczne konfiguracje oprogramowania
- Brak przetwarzania danych produkcyjnych w środowisku testowym
- Separacja klientów (przynajmniej logiczna)
- Dane klientów są przetwarzane wyłącznie w celach określonych w umowie
- Szyfrowanie
- Sieci wydzielone

e) Anonimizacja / pseudonimizacja danych osobowych

W razie potrzeby wdrażane są następujące środki, aby zapobiec przypisywaniu danych osobowych do konkretnego podmiotu danych bez użycia dodatkowych informacji.

- Dane osobowe muszą zostać usunięte lub zanonimizowane / pseudonimizowane po upływie ustawowego okresu przechowywania, jeśli usunięcie nie jest możliwe.
- Funkcje anonimizacji / pseudonimizacji danych
- Zakaz rejestrowania danych dotyczących adresów IP lub innych metadanych osób informujących o nieprawidłowościach
- Bezpieczna i, w razie potrzeby, anonimowa komunikacja z osobami zgłaszającymi nieprawidłowości

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. Integralność

zgodnie z Art. 32 par. 1 lit. b EU GDPR

a) Kontrola transferu danych

Wdrażane są następujące środki integralności danych, które zasadniczo pomagają chronić przed nieuprawnionym lub niezgodnym z prawem przetwarzaniem, zniszczeniem lub przypadkowym uszkodzeniem.

- Szyfrowane połączenia do przesyłania danych
- Dokumentacja dotycząca odbiorców danych oraz czasu trwania planowanych okresów przekazywania lub usuwania danych
- Rejestrowanie transmisji danych
- Wykorzystanie technologii VPN
- Zarządzanie kluczami i proces zarządzania dostępem
- Polityka firmy
- Uwierzytelnianie wieloczynnikowe
- Przetwarzanie danych poza urzędami ściśle uregulowane
- Przepisy bezpieczeństwa dotyczące przechowywania nośników danych
- Niszczenie nośników danych przez certyfikowaną firmę
- Należyta staranność przy wyborze firm transportowych
- Bezpieczne pojemniki transportowe

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) Sterowanie wejściem

W celu zapewnienia możliwości sprawdzenia, przez kogo dane osobowe zostały wprowadzone, zmienione lub usunięte, wdrożono następujące środki.

- Techniczne rejestrowanie wprowadzania, modyfikacji i usuwania danych
- Przydzielanie praw do wprowadzania, zmiany i usuwania danych w oparciu o koncepcję autoryzacji
- Przegląd protokołów
- Możliwość śledzenia wprowadzania, zmiany, usuwania poprzez indywidualne nazwy użytkowników
- Jasno określona odpowiedzialność za usuwanie danych
- Przechowywanie formularzy, z których dane zostały przekazane do zautomatyzowanych operacji przetwarzania

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. Dostępność i odporność

zgodnie z Art. 32 par. 1 lit. b EU GDPR

a) Kontrola dostępności

W celu zapewnienia ochrony danych osobowych przed zniszczeniem lub utratą zostały wdrożone następujące środki:

- Systemy wykrywania ognia i dymu
- Koncepcja nagłych wypadków i bezpieczeństwa
- Gaśnice i klimatyzacja w serwerowniach
- Przegląd procesu tworzenia kopii zapasowych
- Zasilanie bezprzerwowe
- Koncepcja ochrony przed wirusami
- Monitorowanie temperatury i wilgotności w serwerowniach
- Nadmiarowość ważnych elementów systemu
- Regularna kontrola i konserwacja wszystkich systemów

b) Odzyskiwalność

W celu zapewnienia możliwości szybkiego odzyskania danych osobowych stosowane są następujące środki:

- Redundantna infrastruktura
- Regularne kopie zapasowe
- Regularne i zaszyfrowane kopie zapasowe danych klientów
- przechowywanie kopii zapasowych poza siedzibą firmy
- Regularne sprawdzanie kopii zapasowych pod kątem dostępności, kompletności i integralności

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. Procedury regularnego testowania, oceny i ewaluacji

zgodnie z Art. 32 par. 1 lit. d DSGVO i Art. 25 par. 1 DSGVO

a) Zarządzanie ochroną danych

- Mianowany inspektor ochrony danych
- Certyfikaty bezpieczeństwa zgodne z normą ISO 27001
- Wykorzystanie rozwiązań programowych do zarządzania ochroną danych
- Regularne szkolenia pracowników i zobowiązanie wszystkich pracowników do zachowania poufności
- Domyślna ochrona prywatności
- Certyfikaty ochrony danych dla wybranych produktów EQS Group
- Weryfikacja skuteczności technicznych środków bezpieczeństwa, np. za pomocą regularnych audytów
- Polityka firmy w zakresie ochrony danych osobowych
- Centralna dokumentacja wszystkich procedur i regulacji dotyczących ochrony danych osobowych z dostępem dla pracowników zgodnie z potrzebami / uprawnieniami
- W razie potrzeby, przeprowadzenie oceny skutków dla ochrony danych zgodnie z art. 35 EU GDPR
- Udokumentowana koncepcja bezpieczeństwa
- udokumentowane procesy postępowania w przypadku incydentów związanych z ochroną danych oraz wniosków osób, których dane dotyczą

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) Zarządzanie reagowaniem na incydenty

- Udokumentowany proces wykrywania i zgłaszania incydentów bezpieczeństwa / naruszeń danych
- System wykrywania włamań (IDS)
- Oprogramowanie antywirusowe
- Zapory sieciowe
- Dokumentacja incydentów bezpieczeństwa i naruszeń danych jako część systemu zarządzania bezpieczeństwem informacji
- Formalny proces i obowiązki w zakresie działań następczych w odniesieniu do incydentów naruszenia bezpieczeństwa i naruszenia danych

c) System zarządzania bezpieczeństwem informacji

- Wewnętrzny specjalista ds. bezpieczeństwa informacji (CISO)
  Adres e-mail: infosec@eqs.com
- Certyfikaty bezpieczeństwa zgodne z normą ISO 27001
- Regularny przegląd skuteczności technicznych środków bezpieczeństwa
  - System zarządzania bezpieczeństwem informacji (ISMS)

d) Sterowanie procesorem

- Staranny wybór i monitorowanie podwykonawców, z uwzględnieniem aspektów bezpieczeństwa informacji
- Zawarta umowa o przetwarzaniu danych
- Regularny przegląd wykonania umowy
- Niszczenie danych po zakończeniu umowy
  - Uregulowane korzystanie z usług dalszych podwykonawców

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