Tekniske og organisatoriske foranstaltninger for EQS Cloud Services

i henhold til art. 32 EU GDPR (tosproget udgave danish / engelsk)

TOMs_EQS Cloud Services_da-en- Status 29/08/2024

Forord

Dette dokument er udarbejdet på både dansk og engelsk. I tilfælde af uoverensstemmelse gælder den engelske version, som er bindende for parterne.

Dette dokument dækker de tekniske og organisatoriske sikkerhedsforanstaltninger (TOM), som EQS Group har truffet i henhold til art. 32 EU GDPR som følge af den databehandling, der er beskrevet i den underliggende aftale. Følgende TOM gælder generelt for alle EQS Groups Cloud-tjenester.

Organisationer, der selv eller på deres vegne indsamler, behandler eller anvender personoplysninger, skal træffe passende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et passende beskyttelsesniveau.

EQS Group opfylder dette krav ved hjælp af følgende foranstaltninger.

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.

Indhold

1. Generelt

Databeskyttelsesansvarlig:
Oliver Kunert,
Ekstern databeskyttelsesansvarlig
Sunny Systems GmbH
Kontaktoplysninger: dataprotection@eqs.com
Formelt udnævnt den: 15.12.2015
Stilling i virksomheden: Direkte underlagt direktionen

Med jævne mellemrum - mindst en gang om året - gennemføres interne revisioner eller suppleringer af den eksisterende revision, og alle tekniske og organisatoriske sikkerhedsforanstaltninger kontrolleres og opdateres om nødvendigt.

Alle medarbejdere bliver instrueret i kravene til databeskyttelse, når de ansættes. Alle medarbejdere modtager undervisning om databeskyttelse, enten personligt af databeskyttelsesrådgiveren eller via et onlineværktøj.

EQS Group AG har implementeret et informationssikkerhedsstyringssystem og er certificeret i henhold til ISO 27001.

Bemærk venligst, at nylige opkøb muligvis ikke implementerer alle nedenstående kontroller og i øjeblikket ikke er en del af vores informationssikkerhedsstyringssystem. EQS arbejder dog på at implementere disse kontroller og inkludere nylige opkøb i certificeringsomfanget til sin tid.

Desuden kan banebrydende teknologier, som f.eks. funktionalitet, der involverer »generativ AI«,

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.

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

muligvis ikke implementere alle nedenstående kontroller, da der gælder begrænsninger hos vores leverandører.

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. Fortrolighed

i henhold til art. 32, stk. 1 lit. b EU GDPR

a) Fysisk adgangskontrol

Følgende foranstaltninger er blevet gennemført for at begrænse eller forhindre uautoriseret adgang til lokaler, hvor der behandles personoplysninger, eller for at forhindre uautoriseret adgang.

- Meget sikre og ISO 27001-certificerede datacentre
- Alarmsystem og/eller sikkerhedstjeneste
- Sikkerhedslåse
- Nøglehåndtering
- Adgang kun for autoriserede medarbejdere
- Definition af sikkerhedszoner med stærkt begrænsede adgangsrettigheder ("Needs-Access"-princippet)
- Automatiserede fysiske adgangskontrolsystemer (f.eks. chipkort eller transpondersystemer)
- Kontrol af besøgende (logning og ledsagelse af besøgende)
- Ingen adgang uden ledsagelse for eksterne personer til serverrum
- Obligatoriske virksomhedsretningslinjer for alle medarbejdere
- Omhyggelig udvælgelse af eksternt personale og tjenesteydere

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) Logisk adgangskontrol

Følgende foranstaltninger er blevet implementeret for at forhindre, at EQS Group's databehandlingsfaciliteter kan bruges af uautoriserede personer.

- Anti-virus-software på server og klient
- Adskillelse af administrative konti og brugerkonti
- Firewalls
- Regler og politik for adgangskoder (kompleksitet, længde og udløbsdato)
- VPN til fjernadgang
- "Politik for et rent skrivebord / en ren skærm
- Automatisk skrivebordslås
- Administration og regelmæssig gennemgang af brugertilladelser
- Kryptering af (eksterne) databærere, smartphones og notebooks/tablets
- Tildeling af tilladelser i henhold til "need-to-know"-princippet
- Indtrængningsdetektionssystemer
- Retningslinjer for databeskyttelse og it-sikkerhed

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) Kontrol af dataadgang

Følgende foranstaltninger er blevet gennemført for at sikre, at personoplysninger kun kan tilgås i overensstemmelse med de tildelte tilladelser. Desuden er det sikret, at personoplysninger ikke kan behandles uden tilladelse, dvs. at de ikke kan registreres, læses, kopieres, ændres eller slettes uden tilladelse.

- Autorisationskoncept med differentieret autorisationstildeling
- Antallet af administrative brugere er begrænset til et nødvendigt minimum
- Logning af adgang til applikationer, især ved indtastning, ændring og sletning af data
- Administrators forvaltning af brugerrettigheder
- Identifikation og autentificering af brugere
- Autorisations- og adgangsregler
- Kryptering i bevægelse og i hvile
- Låsning af følsomme personlige data og fortrolige oplysninger
- Makuleringsmaskine i henhold til DIN 66399 eller ekstern tjenesteudbyder til destruktion af data
- Skriftlige regler for håndtering af elektronisk betjeningsudstyr

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) Kontrol af adskillelse

Følgende foranstaltninger er blevet gennemført for at sikre, at data, der indsamles til forskellige formål, behandles separat.

- Adskillelse af produktions- og testmiljø
- Begrebet autorisation for adgang til data
- Sikre softwarekonfigurationer
- Ingen behandling af produktive data i testmiljøet
- Kundeadskillelse (i det mindste logisk adskillelse)
- Kundeoplysninger behandles kun til de kontraktligt definerede formål
- Kryptering
- Adskilte net

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) Anonymisering / pseudonymisering af personoplysninger

Om nødvendigt gennemføres følgende foranstaltninger for at forhindre, at personoplysninger kan henføres til en bestemt registreret person uden brug af yderligere oplysninger.

- Personoplysninger skal slettes eller anonymiseres / pseudonymiseres efter udløbet af den lovbestemte opbevaringsperiode, hvis det ikke er muligt at slette dem.
- Funktioner til anonymisering / pseudonymisering af data
- Ingen logning af IP-adresser eller andre metadata om whistleblowere
- Sikker og, hvis det ønskes, anonym kommunikation med whistleblowere

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. Integritet

i henhold til art. 32, stk. 1 lit. b EU GDPR

a) Kontrol af dataoverførsel

Følgende foranstaltninger til sikring af dataintegritet er gennemført, som generelt bidrager til at beskytte mod uautoriseret eller ulovlig behandling, ødelæggelse eller utilsigtet beskadigelse.

- Krypterede forbindelser til overførsel af data
- Dokumentation af datamodtagerne og varigheden af de planlagte overførsels- eller sletningsperioder
- Logning af dataoverførslen
- Brug af VPN-teknologi
- Nøgle- og adgangsstyringsproces
- Virksomhedspolitik
- Multifaktor-autentifikation
- Behandling af oplysninger uden for kontorerne er strengt reguleret
- Sikkerhedsbestemmelser for opbevaring af datamedier
- Destruktion af datamedier af certificeret virksomhed
- Omhyggelighed ved udvælgelse af transportvirksomheder
- Sikre transportcontainere

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) Indgangskontrol

Følgende foranstaltninger er blevet gennemført for at sikre, at det er muligt at kontrollere, hvem der har indtastet, ændret eller fjernet personoplysninger.

- Teknisk logning af indtastning, ændring og sletning af data
- Tildeling af rettigheder til at indtaste, ændre og slette data på grundlag af et autoriseringskoncept
- Gennemgang af protokoller
- Sporbarhed af input, ændringer og sletning via individuelle brugernavne
- Klare ansvarsområder for sletninger
- Opbevaring af formularer, hvorfra oplysninger er blevet overført til automatiserede behandlinger

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. Tilgængelighed og modstandsdygtighed

i henhold til art. 32, stk. 1 lit. b EU GDPR

a) Kontrol af tilgængelighed

Følgende foranstaltninger er blevet gennemført for at sikre, at personoplysninger er beskyttet mod ødelæggelse eller tab:

- Brand- og røgdetektionssystemer
- Nød- og sikkerhedskoncept
- Brandslukkere og klimaanlæg i serverrum
- Gennemgang af backup-processen
- Afbrydelsesfri strømforsyning
- Virusbeskyttelseskoncept
- Overvågning af temperatur og luftfugtighed i serverrum
- Redundans af vigtige systemkomponenter
- Regelmæssig kontrol og vedligeholdelse af alle systemer

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) Genindvindingsmuligheder

Følgende foranstaltninger gennemføres for at sikre, at personoplysninger hurtigt kan gendannes:

- Redundant infrastruktur
- Regelmæssige sikkerhedskopier
- Regelmæssige og krypterede sikkerhedskopier af kundedata
- Ekstern backup-opbevaring
- Regelmæssig kontrol af sikkerhedskopier for tilgængelighed, fuldstændighed og integritet

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. Procedurer for regelmæssig afprøvning, vurdering og evaluering

i henhold til art. 32, stk. 1 lit. d GDPR og art. 25 stk. 1 GDPR

a) Forvaltning af databeskyttelse

- Udpeget databeskyttelsesrådgiver
- Sikkerhedscertificeringer i henhold til ISO 27001
- Brug af softwareløsninger til forvaltning af databeskyttelse
- Regelmæssig uddannelse af medarbejdere og alle medarbejderes forpligtelse til at overholde fortrolighed
- Privatliv som standard
- Databeskyttelsescertificeringer for udvalgte produkter fra EQS Group AG
- Kontrol af de tekniske sikkerhedsforanstaltningers effektivitet, f.eks. ved hjælp af regelmæssig revision
- Virksomhedens politik om databeskyttelse
- Central dokumentation af alle procedurer og bestemmelser om databeskyttelse med adgang for medarbejdere efter behov/autorisation
- Om nødvendigt gennemførelse af en konsekvensanalyse af databeskyttelsen i henhold til artikel. 35 EU GDPR
- Dokumenteret sikkerhedskoncept
- Dokumenterede processer til håndtering af databeskyttelseshændelser samt anmodninger fra registrerede personer
- Procesos documentados para gestionar los incidentes de protección de datos, así como las solicitudes de los interesados

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) Forvaltning af hændelsesrespons

- Dokumenteret proces til at opdage og rapportere sikkerhedshændelser / databrud
- Indtrængningsdetektionssystem (IDS)
- Antivirus-software
- Firewalls
- Dokumentation af sikkerhedshændelser og databrud som en del af informationssikkerhedsstyringssystemet
- Formel proces og ansvar for opfølgning af sikkerhedshændelser og databrud

c) Forvaltningssystem for informationssikkerhed

- Intern informationssikkerhedsansvarlig (CISO), E-mail: infosec@eqs.com
- Sikkerhedscertificeringer i henhold til ISO 27001
- Regelmæssig gennemgang af de tekniske sikkerhedsforanstaltningers effektivitet
- Forvaltningssystem for informationssikkerhed (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) Processorstyring

- Omhyggelig udvælgelse og overvågning af underleverandører under hensyntagen til informationssikkerhedsaspekter
- Indgået databehandleraftale
- Regelmæssig gennemgang af kontraktens gennemførelse
- Destruktion af data efter kontraktens udløb
- Reguleret brug af yderligere underleverandører

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