Medidas técnicas y organizativas para EQS Cloud Services

de acuerdo con el Art. 32 EU GDPR (versión bilingüe español / inglés)

TOMs_EQS Cloud Services_es-en- Status 31/10/2024

Prólogo

Este documento ha sido preparado tanto en español como en inglés. En caso de contradicción, se aplicará la versión inglesa y será vinculante para las partes.

Este documento cubre las medidas de seguridad técnicas y organizativas (TOM) adoptadas por EQS Group en el sentido del Art. 32 del GDPR de la UE resultantes del procesamiento de datos descrito en el Acuerdo subyacente. Las siguientes TOM se aplican de forma general a todos los servicios en la nube del EQS Group.

Las organizaciones que recojan, traten o utilicen datos personales por sí mismas o en su nombre deben adoptar las medidas de seguridad técnicas y organizativas apropiadas para garantizar un nivel de protección adecuado.

EQS Group cumple este requisito con las siguientes medidas.

Foreword

This document has been prepared in both Spanish 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.

Contenido

1. General

Responsable de la protección de datos:
Oliver Kunert,
DPO externo Sunny Systems GmbH
Datos de contacto:
dataprotection@eqs.com
Nombrado formalmente el: 15.12.2015
Posición en la empresa: Depende directamente del Consejo de Administración

A intervalos regulares -al menos una vez al año- se realizan auditorías internas o complementos de la auditoría existente y se comprueban todas las medidas de seguridad técnicas y organizativas y se actualizan si es necesario.

Todos los empleados son instruidos en los requisitos de protección de datos en el momento de su contratación. Todos los empleados reciben formación sobre protección de datos, ya sea en persona por el responsable de protección de datos o a través de una herramienta en línea.

EQS Group ha implantado un sistema de gestión de la seguridad de la información y está certificado según la norma ISO 27001.

Por favor, tenga en cuenta que las adquisiciones recientes pueden no implementar todos los controles indicados a continuación y que actualmente estos no forman parte de nuestro sistema de gestión de seguridad de la información. Sin embargo, EQS está trabajando para implementar estos controles e incluir las adquisiciones recientes

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.

en el alcance de la certificación en su debido momento.

Además, las tecnologías de vanguardia, como la funcionalidad que implica "IA Generativa", pueden no implementar todos los controles mencionados a continuación, ya que se aplican las limitaciones de nuestros Proveedores.

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. Confidencialidad

de acuerdo con el Art. 32 para. 1 lit. EU GDPR

a) Control de acceso físico

Se han aplicado las siguientes medidas para restringir o impedir el acceso no autorizado a los locales donde se procesan los datos personales.

- Centros de datos altamente seguros y con certificación ISO 27001
- Sistema de alarma y/o servicio de seguridad
- Cerraduras de seguridad
- Gestión de claves
- Acceso sólo para empleados autorizados
- Definición de zonas de seguridad con derechos de acceso muy restringidos (principio de "necesidad de acceso")
- Sistemas automatizados de control de acceso físico (por ejemplo, tarjetas con chip o sistemas de transpondedor)
- Control de visitantes (registro y acompañamiento de visitantes)
- No se permite el acceso sin escolta de personas externas a las salas de servidores
- Directrices corporativas obligatorias para todos los empleados
- Selección cuidadosa del personal externo y de los proveedores de servicios

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) Control de acceso lógico

Se han implementado las siguientes medidas para evitar que las instalaciones de procesamiento de datos de EQS Group sean utilizadas por personas no autorizadas.

- Software antivirus en el servidor y en el cliente
- Separación de las cuentas administrativas y de usuario
- Cortafuegos
- Normas y política de contraseñas (complejidad, longitud y caducidad)
- VPN para acceso remoto
- "Política de escritorio limpio / pantalla despejada
- Bloqueo automático del escritorio
- Administración y revisión periódica de las autorizaciones de los usuarios
- Cifrado de soportes de datos (externos), smartphones y portátiles/tabletas
- Asignación de autorizaciones según el principio de "necesidad de conocer"
- Sistemas de detección de intrusos
- Directrices sobre protección de datos y seguridad informática

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) Control de acceso a los datos

Se han aplicado las siguientes medidas para garantizar que sólo se pueda acceder a los datos personales de acuerdo con las autorizaciones asignadas. Además, se garantiza que los datos personales no puedan ser tratados sin autorización, es decir, que no puedan ser registrados, leídos, copiados, modificados o eliminados sin autorización.

- Concepto de autorización con asignación de autorización diferenciada
- Número de usuarios administrativos limitado al mínimo necesario
- Registro de los accesos a las aplicaciones, concretamente al introducir, modificar y borrar datos
- Gestión de los derechos de los usuarios por parte de los administradores
- Identificación y autenticación de usuarios
- Normas de autorización y acceso
- Cifrado en movimiento y en reposo
- Bloqueo de datos personales sensibles e información confidencial
- Destructora de archivos según la norma DIN 66399 o proveedor de servicios externo para la destrucción de datos
- Normas escritas para el manejo de dispositivos electrónicos de funcionamiento

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) Control de separación

Se han aplicado las siguientes medidas para garantizar que los datos recogidos para diferentes fines se traten por separado.

- Separación del entorno productivo y de prueba
- Concepto de autorización para el acceso a los datos
- Configuraciones de software seguras
- No se procesan los datos productivos en el entorno de prueba
- Separación de los clientes (al menos separación lógica)
- Los datos de los clientes sólo se procesan para los fines definidos contractualmente
- Codificación
- Redes separadas

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) Anonimización / seudonimización de datos personales

Cuando sea necesario, se aplicarán las siguientes medidas para evitar que los datos personales se atribuyan a un sujeto específico sin el uso de información adicional.

- Los datos personales deben ser eliminados o anonimizados/pseudonimizados después de la expiración del período de conservación legal si la eliminación no es posible.
- Funciones de anonimización/pseudonimización de datos
- No se registran los datos de las direcciones IP ni otros metadatos de los chivatos
- Comunicación segura y, si se desea, anónima con los chivatos

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. Integridad

de acuerdo con el Art. 32 para. 1 lit. b EU GDPR

a) Control de transferencia de datos

Se aplican las siguientes medidas de integridad de los datos, que en general ayudan a protegerlos contra el tratamiento no autorizado o ilegal, la destrucción o el daño accidental.

- Conexiones cifradas para la transmisión de datos
- Documentación de los destinatarios de los datos y de la duración de los períodos de transferencia o supresión previstos
- Registro de la transmisión de datos
- Uso de la tecnología VPN
- Proceso de gestión de claves y accesos
- Política de la empresa
- Autenticación multifactorial
- Tratamiento de datos fuera de las oficinas estrictamente regulado
- Disposiciones de seguridad para el almacenamiento de soportes de datos
- Destrucción de soportes de datos por parte de una empresa certificada
- Diligencia debida en la selección de empresas de transporte
- Contenedores de transporte seguros

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) Control de entrada

Se han aplicado las siguientes medidas para garantizar que sea posible verificar por quién se han introducido, modificado o eliminado los datos personales.

- Registro técnico de la introducción, modificación y supresión de datos
- Asignación de derechos de introducción, modificación y supresión de datos basada en un concepto de autorización
- Revisión de los protocolos
- Trazabilidad de las entradas, modificaciones y supresiones a través de los nombres de usuario individuales
- Responsabilidades claras para las supresiones
- Conservación de los formularios cuyos datos se han transferido a operaciones de tratamiento automatizado

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. Disponibilidad y resistencia

de acuerdo con el Art. 32 para. 1 lit. b EU GDPR

a) Control de disponibilidad

Se han aplicado las siguientes medidas para garantizar la protección de los datos personales contra su destrucción o pérdida:

- Sistemas de detección de incendios y humos
- Concepto de emergencia y seguridad
- Extintores y aire acondicionado en las salas de servidores
- Revisión del proceso de copia de seguridad
- Sistema de alimentación ininterrumpida
- Concepto de protección antivirus
- Control de la temperatura y la humedad en las salas de servidores
- Redundancia de componentes importantes del sistema
- Control y mantenimiento regular de todos los sistemas

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) Recuperabilidad

Las siguientes medidas se aplican para garantizar la rápida recuperación de los datos personales:

- Infraestructura redundante
- Copias de seguridad periódicas
- Copias de seguridad periódicas y cifradas de los datos de los clientes
- Almacenamiento de copias de seguridad fuera de las instalaciones
- Comprobación periódica de la disponibilidad, la exhaustividad y la integridad de las copias de seguridad

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. Procedimientos para la realización de pruebas periódicas, evaluación y valoración

de acuerdo con el Art. 32 para. 1 lit. d y Art. 25 para. 1 EU GDPR

a) Gestión de la protección de datos

- Nombrado responsable de la protección de datos
- Certificaciones de seguridad según la norma ISO 27001
- Uso de soluciones informáticas para la gestión de la protección de datos
- Formación periódica de los empleados y compromiso de todos ellos con la confidencialidad
- Privacidad por defecto
- Certificaciones de protección de datos para productos seleccionados de EQS Group
- Verificación de la eficacia de las medidas técnicas de seguridad, por ejemplo, mediante auditorías periódicas
- Política de la empresa en materia de protección de datos
- Documentación central de todos los procedimientos y reglamentos sobre protección de datos con acceso para los empleados según la necesidad / autorización
- Si es necesario, la aplicación de la evaluación de impacto de la protección de datos de acuerdo con el Art. 35 EU GDPR
- Concepto de seguridad documentado

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

› Procesos documentados para gestionar los incidentes de protección de datos, así como las solicitudes de los interesados

› Documented processes for handling data protection incidents as well as data subject requests

b) Gestión de la respuesta a incidentes

- Proceso documentado para detectar y notificar incidentes de seguridad / violaciones de datos
- Sistema de detección de intrusos (IDS)
- Software antivirus
- Cortafuegos
- Documentación de incidentes de seguridad y violaciones de datos como parte del sistema de gestión de la seguridad de la información
- Proceso y responsabilidades formales para el seguimiento de incidentes de seguridad y violaciones de datos

c) Sistema de gestión de la seguridad de la información

- Responsable interno de seguridad de la información (CISO) - Dirección de correo electrónico: infosec@eqs.com
- Certificaciones de seguridad según la norma ISO 27001
- Revisión periódica de la eficacia de las medidas técnicas de seguridad
- Sistema de gestión de la seguridad de la información (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) Control del procesador

- Selección y supervisión cuidadosa de los subcontratistas, teniendo en cuenta los aspectos de seguridad de la información
- Acuerdo de procesamiento de datos concluido
- Revisión periódica de la ejecución del contrato
- Destrucción de datos tras la finalización del contrato
- Uso regulado de otros subcontratistas

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