» Medidas técnicas e organizacionais para EQS Cloud Services «

de acordo com o Art. 32 RGPD UE (versão bilingue português / inglês)

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

Prefácio

Este documento foi preparado tanto em português como em inglês. Em caso de qualquer inconsistência, a versão inglesa é aplicável e vinculativa para as partes.

Este documento cobre as medidas de segurança técnica e organizacional (TOMs) tomadas pelo EQS Group na acepção do Art. 32 RGPD UE resultantes do processamento de dados descrito no Acordo subjacente. Os seguintes TOMs aplicam-se geralmente a todos os serviços em nuvem do EQS Group.

As organizações que recolhem, processam ou utilizam dados pessoais, elas próprias ou em seu nome, devem tomar as medidas de segurança técnicas e organizacionais adequadas para garantir um nível de protecção adequado.

O EQS Group cumpre este requisito através das seguintes medidas.

Foreword

This document has been prepared in both Portuguese 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.

Conteúdo

1. Geral

Responsável pela protecção de dados:
Oliver Kunert,
DPO externo Sunny Systems GmbH
Detalhes de contacto:
dataprotection@eqs.com
Formalmente nomeado em a: 15.12.2015
Posição na empresa: Responde diretamente à Diretoria Executiva

A intervalos regulares - pelo menos uma vez por ano - são realizadas auditorias internas ou suplementos à auditoria existente e todas as medidas de segurança técnica e organizacional são verificadas e actualizadas, se necessário.

Todos os empregados são instruídos sobre os requisitos de proteção de dados quando são contratados. Cada empregado recebe treinamento sobre proteção de dados, pessoalmente pelo responsável pela proteção de dados ou através de uma ferramenta on-line.

O EQS Group AG implementou um sistema de gestão de segurança da informação e é certificado de acordo com a norma 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. Confidencialidade

de acordo com o Art. 32 parágrafo. 1 lit. b RGPD UE

a) Controle de acesso físico

As seguintes medidas foram implementadas para restringir ou impedir o acesso não autorizado às instalações onde os dados pessoais são processados.

- Centros de dados altamente seguros e certificados pela ISO 27001
- Sistema de alarme e/ou serviço de segurança
- Fechaduras de segurança
- Gestão de chaves
- Acesso apenas para funcionários autorizados
- Definição de zonas de segurança com direitos de acesso altamente restritos (princípio "Needs-Access")
- Sistemas automatizados de controlo de acesso físico (por exemplo, cartões chip ou sistemas de transponder)
- Controlo de visitantes (registo e escolta de visitantes)
- Sem acesso sem escolta para pessoas externas às salas do servidor
- Diretrizes corporativas obrigatórias para todos os funcionários
- Seleção cuidadosa de pessoal externo e prestadores de serviços

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) Controle de acesso lógico

As seguintes medidas foram implementadas para evitar que as instalações de processamento de dados do EQS Group AG sejam utilizadas por pessoas não autorizadas.

- Software anti-vírus em servidor e cliente
- Separação das contas administrativas e de usuário
- Firewalls
- Regras e política de senha (complexidade, duração e expiração)
- VPN para acesso remoto
- "Clean Desk / Clear Screen Policy"
- Bloqueio automático da área de trabalho
- Administração e revisão regular das autorizações dos usuários
- Criptografia de suportes de dados (externos), smartphones e notebooks/computadores
- Atribuição de autorizações de acordo com o princípio "need-to-know"
- Sistemas de detecção de intrusão
- Diretrizes sobre proteção de dados e segurança de TI

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) Controle de acesso aos dados

As seguintes medidas foram implementadas para garantir que os dados pessoais só possam ser acessados de acordo com as autorizações atribuídas. Além disso, é garantido que os dados pessoais não podem ser processados sem autorização, ou seja, não podem ser registrados, lidos, copiados, modificados ou eliminados sem autorização.

- Conceito de autorização com atribuição de autorização diferenciada
- Número de usuários administrativos limitado a um mínimo necessário
- Registo de acessos a aplicações, especificamente na entrada, alteração e eliminação de dados
- Gestão dos direitos dos utilizadores pelos administradores
- Identificação e autenticação do usuário
- Regras de autorização e acesso
- Criptografia em movimento e em repouso
- Bloqueio de dados pessoais sensíveis e informações confidenciais
- Trituradora de arquivos de acordo com DIN 66399 ou prestador de serviços externo para destruição de dados
- Regulamentos escritos para o manuseio de dispositivos eletrônicos de operação

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) Controle de separação

As seguintes medidas foram implementadas para garantir que os dados recolhidos para diferentes fins sejam processados separadamente.

- Separação do ambiente produtivo e de teste
- Conceito de autorização para acesso aos dados
- Configurações de software seguras
- Nenhum processamento de dados produtivos em ambiente de teste
- Separação de clientes (pelo menos separação lógica)
- Os dados do cliente só são processados para os fins contratualmente definidos
- Criptografia
- Redes separadas

e) Anonimização / pseudonimização de dados pessoais

Sempre que necessário, são implementadas as seguintes medidas para evitar que os dados pessoais sejam atribuídos a um determinado indivíduo sem o uso de informações adicionais.

- Os dados pessoais devem ser apagados ou anonimizados / pseudonimizados após a expiração do período de retenção legal, se não for possível apagá-los.
- Funções para anonimização / pseudonimização de dados
- Sem registro de dados de endereço IP ou outros metadados de informadores
- Comunicação segura e, se desejado, anónima com informadores

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. Integridade

de acordo com o Art. 32 parágrafo. 1 lit. b RGPD UE

a) Controle de transferência de dados

As seguintes medidas de integridade de dados são implementadas, que geralmente ajudam a proteger contra processamento não autorizado ou ilegal, destruição ou danos acidentais.

- Conexões criptografadas para a transmissão de dados
- Documentação dos destinatários dos dados e a duração dos períodos de transferência ou eliminação planejados
- Registo da transmissão de dados
- Utilização da tecnologia VPN
- Gestão de chaves e processo de gestão de acesso
- Política da empresa
- Autenticação multi-factor
- Tratamento de dados fora dos escritórios estritamente regulamentados
- Disposições de segurança para o armazenamento de suportes de dados
- Destruição de suportes de dados por empresa certificada
- Due diligence na selecção de empresas de transporte
- Contentores 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) Controlos das entradas

As seguintes medidas foram implementadas para assegurar que é possível verificar por quem os dados pessoais foram introduzidos, modificados ou removidos.

- Registo técnico da entrada, modificação e eliminação de dados
- Atribuição de direitos para entrar, modificar e eliminar dados com base em um conceito de autorização
- Revisão de protocolos
- Rastreabilidade de entrada, alteração, eliminação através de nomes de utilizador individuais
- Responsabilidades claras pelas eliminações
- Retenção de formulários a partir dos quais os dados foram transferidos para operações de processamento 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. Disponibilidade e resiliência

de acordo com o Art. 32 parágrafo. 1 lit. b RGPD UE

a) Controle de disponibilidade

As seguintes medidas foram implementadas para assegurar que os dados pessoais sejam protegidos contra a destruição ou perda:

- Sistemas de detecção de incêndio e fumaça
- Conceito de emergência e segurança
- Extintores de incêndio e ar condicionado nas salas dos servidores
- Revisão do processo de backup
- Alimentação ininterrupta de energia
- Conceito de proteção contra vírus
- Monitorização da temperatura e humidade nas salas dos servidores
- Redundância de componentes importantes do sistema
- Controle e manutenção regular de todos os sistemas

b) Recuperabilidade

As seguintes medidas são implementadas para garantir que os dados pessoais possam ser recuperados rapidamente:

- Infra-estrutura redundante
- Cópias de segurança regulares
- Backups regulares e criptografados dos dados dos clientes
- Armazenamento de backup externo
- Verificação regular de backups para disponibilidade, completude e integridade

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. Procedimentos para a realização de testes, avaliação e análise regulares

de acordo com o Art. 32 parágrafo. 1 lit. d RGPD UE e Art. 25, parágrafo. 1 RGPD UE

a) Gestão da protecção de dados

- Responsável pela protecção de dados nomeado
- Certificações de segurança de acordo com a ISO 27001
- Utilização de soluções de software para a gestão da protecção de dados
- Formação regular dos colaboradores e compromisso de todos os colaboradores com a confidencialidade
- Privacidade por defeito
- Certificações de protecção de dados para produtos seleccionados da EQS Group AG
- Verificação da eficácia das medidas técnicas de segurança, por exemplo, por meio de auditorias regulares
- Política da empresa em matéria de protecção de dados
- Documentação central de todos os procedimentos e regulamentos sobre proteção de dados com acesso para os funcionários de acordo com a necessidade / autorização
- Se necessário, implementação da avaliação do impacto da protecção de dados de acordo com o Art. 35 RGPD UE
- Conceito de segurança documentado
- Processos documentados para o tratamento de incidentes de protecção de dados, bem como pedidos de pessoas em causa

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) Gestão da resposta a incidentes

› Processo documentado para a detecção e comunicação de incidentes de segurança / violações de dados
› Sistema de detecção de intrusão (IDS)
› Software antivírus
› Firewalls
› Documentação de incidentes de segurança e violações de dados como parte do sistema de gestão de segurança da informação
› Processo formal e responsabilidades pelo acompanhamento de incidentes de segurança e violações de dados

c) Sistema de gestão da segurança da informação

› Responsável interno pela segurança da informação (CISO)
Endereço de e-mail: infosec@eqs.com
› Certificações de segurança de acordo com a ISO 27001
› Revisão regular da eficácia das medidas técnicas de segurança
› Sistema de gestão da segurança da informação (ISMS)

d) Controle de processadores

› Seleção e monitoramento cuidadoso dos subempreiteiros, considerando aspectos de segurança da informação
› Contrato de processamento de dados concluído
› Revisão regular da execução do contrato
› Destruição de dados após o final do contrato
› Utilização regulada de outros subempreiteiros

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