EQS GROUP

Technische und organisatorische Maßnahmen für EQS Cloud Services

nach Art. 32 EU-DSGVO

TOMs_EQS Cloud Services_de - Status 02/09/2024

Vorwort

Dieses Dokument umfasst die von der EQS Group AG getroffenen technischen und organisatorischen Schutzmaßnahmen i.S.d. Art. 32 EU-DSGVO, die sich aus der im Hauptvertrag beschriebenen Datenverarbeitung ergeben. Die folgenden TOMs gelten allgemein für alle Cloud Services der EQS Group.

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, müssen geeignete technische und organisatorische Maßnahmen ergreifen, um ein angemessenes Schutzniveau zu gewährleisten.

Die EQS Group AG erfüllt diesen Anspruch durch folgende Maßnahmen.

Inhalt:

1. Allgemeines

Datenschutzbeauftragter:	Oliver Kunert, Externer DSB Sunny Systems GmbH
Kontaktdaten:	datenschutz@eqs.com
Schriftliche Bestellung:	15.12.2015
Stellung im Unternehmen:	In seiner Aufgabe direkt der Geschäftsleitung unterstellt

In regelmäßigen Abständen – mindestens jährlich – werden interne Audits bzw. Ergänzungen des bestehenden Audits durchgeführt und dabei alle technischen und organisatorischen Maßnahmen überprüft und ggf. aktualisiert.

Alle Mitarbeiter werden bei der Einstellung in die Anforderungen des Datenschutzes eingewiesen. Jeder Mitarbeiter erhält eine Schulung zum Datenschutz, entweder persönlich durch den Datenschutzbeauftragten oder über ein Onlinetool.

EQS Group AG hat ein Informationssicherheitsmanagementsystem implementiert und ist nach ISO 27001 zertifiziert.

Bitte beachten Sie, dass die jüngsten Akquisitionen möglicherweise nicht alle der unten genannten Kontrollen umsetzen und derzeit nicht Teil unseres Informationssicherheitsmanagementsystems sind. EQS arbeitet jedoch daran, diese Kontrollen zu implementieren und die jüngsten Übernahmen zu gegebener Zeit in den Zertifizierungsumfang aufzunehmen.

Darüber hinaus werden bei Spitzentechnologien, wie z. B. Funktionen, die „generative KI" beinhalten, möglicherweise nicht alle der unten aufgeführten Kontrollen implementiert, da bei unseren Zulieferern Einschränkungen gelten.

2. Vertraulichkeit

gemäß Art. 32 Abs. 1 lit. b EU-DSGVO

a) Zutrittskontrolle

Es sind folgende Maßnahmen umgesetzt, um den Zutritt Unbefugter zu Räumlichkeiten, in denen personenbezogene Daten verarbeitet werden, einzuschränken bzw. zu unterbinden.

- Hochsichere und ISO 27001 zertifizierte Rechenzentren
- Alarmanlage und/oder Sicherheitsdienst
- Sicherheitsschlösser
- Schlüsselmanagement
- Zutritt nur für autorisierte Mitarbeiter
- Definition von Sicherheitszonen mit stark eingeschränkten Zutrittsrechten („Needs-Access"-Prinzip)
- Automatisierte Zutrittskontrollsysteme (z.B. Chipkarten oder Transpondersysteme)
- Besucherkontrolle (Protokollierung und Begleitung der Besucher)
- Kein unbegleiteter Zutritt für Externe zu Serverräumen
- Verpflichtende Unternehmensrichtlinien für alle Mitarbeiter
- Sorgfältige Auswahl externen Personals und externer Dienstleister

b) Zugangskontrolle

Es sind folgende Maßnahmen umgesetzt, die verhindern, dass Datenverarbeitungseinrichtungen der EQS Group AG von Unbefugten benutzt werden können.

- Anti-Viren-Software auf Server und Client
- Trennung von administrativen und Benutzeraccounts
- Firewalls
- Passwortregelungen und Richtlinie (Komplexität, Länge und Wiederverwendung)
- VPN bei Remote Zugriffen
- „Clean Desk / Clear Screen"-Richtlinie
- Automatische Desktopsperre
- Verwaltung und regelmäßige Überprüfung von Benutzerberechtigungen
- Verschlüsselung von (externen) Datenträgern, Smartphones und Notebooks/ Tablets
- Vergabe von Berechtigungen nach dem „Need-to-Know"-Prinzip

- Intrusion Detection Systeme
- Richtlinien zu Datenschutz und IT-Sicherheit

c) Zugriffskontrolle

Es sind folgende Maßnahmen umgesetzt, die gewährleisten, dass Zugriffe auf personenbezogene Daten ausschließlich entsprechend der zugeordneten Berechtigungen möglich sind. Zudem wird sichergestellt, dass personenbezogene Daten nicht unbefugt verarbeitet, d.h. nicht unbefugt erfasst, gelesen, kopiert, verändert oder gelöscht werden können.

- Berechtigungskonzept mit differenzierter Berechtigungsvergabe
- Auf ein nötiges Minimum begrenzte Anzahl an administrativen Benutzern
- Protokollierung von Zugriffen auf Anwendungen, konkret bei Eingabe, Änderung und Löschung von Daten
- Verwaltung der Benutzerrechte durch Administratoren
- Identifikation und Authentifizierung der Benutzer
- Autorisierungs- und Zugriffsregelungen
- Verschlüsselung in motion und at rest
- Verschluss von sensiblen personenbezogenen Daten und vertraulichen Informationen
- Aktenschredder gem. DIN 66399 bzw. externer Dienstleister für Datenvernichtung
- Schriftliche Regelungen für den Umgang mit elektronischen Betriebsgeräten

d) Trennungskontrolle

Es sind folgende Maßnahmen umgesetzt, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

- Trennung von Produktiv- und Testumgebung
- Berechtigungskonzept für den Zugriff auf Daten
- Sichere Softwarekonfigurationen
- Keine Verarbeitung von Produktivdaten in Testumgebung
- Kundentrennung (mindestens logische Trennung)
- Kundendaten werden nur zu den vertraglich festgelegten Zwecken verarbeitet
- Verschlüsselung
- Separierte Netzwerke

e) Anonymisierung / Pseudonymisierung personenbezogener Daten

Sofern erforderlich sind folgende Maßnahmen umgesetzt, um zu verhindern, dass personenbezogene Daten ohne Hinzuziehung zusätzlicher Informationen einer spezifischen betroffenen Person zugeordnet werden können.

- Personenbezogene Daten sind, sofern eine Löschung nicht möglich ist, nach Ablauf der gesetzlichen Speicherungsfrist zu löschen oder zu anonymisieren / pseudonymisieren
- Funktionen zur Anonymisierung / Pseudonymisierung von Daten
- Verzicht auf Protokollierung von IP-Adressdaten oder sonstigen Metadaten von Hinweisgebern
- Sichere und auf Wunsch anonyme Kommunikation mit Hinweisgebern

3. Integrität

gemäß Art. 32 Abs. 1 lit. b EU-DSGVO

a) Weitergabekontrolle

Es sind folgende Maßnahmen zur Gewährleistung der Datenintegrität umgesetzt, die generell zum Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, Zerstörung oder unbeabsichtigter Schädigung beitragen.

- Verschlüsselte Verbindungen zur Übertragung von Daten
- Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
- Protokollierung der Datenübertragung
- Einsatz von VPN-Technologie
- Schlüsselverwaltung und Zutrittsmanagementprozess
- Unternehmensrichtlinien
- Multi-Faktor-Authentifizierung
- Verarbeitung von Daten außerhalb der Büros streng reglementiert
- Sicherheitsbestimmungen für die Aufbewahrung von Datenträgern
- Vernichtung von Datenträgern durch zertifiziertes Unternehmen
- Sorgfalt bei der Auswahl von Transportfirmen
- Sichere Transportbehälter

b) Eingabekontrolle

Es sind folgende Maßnahmen umgesetzt, die gewährleisten, dass überprüft und festgestellt werden kann, von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind.

- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Kontrolle der Protokolle
- Nachvollziehbarkeit von Eingabe, Änderung, Löschung durch individuelle Benutzernamen
- Klare Zuständigkeiten für Löschungen
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden

4. Verfügbarkeit und Belastbarkeit

gemäß Art. 32 Abs. 1 lit. b EU-DSGVO

a) Verfügbarkeitskontrolle

Es sind folgende Maßnahmen umgesetzt, die gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind:

- Feuer- und Rauchmeldeanlagen
- Notfall- und Sicherheitskonzept
- Feuerlöscher und Klimaanlage in Serverräumen
- Kontrolle des Sicherungsvorgangs
- Unterbrechungsfreie Stromversorgung
- Virenschutzkonzept
- Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Redundanz wichtiger Systemkomponenten
- Regelmäßige Kontrolle und Wartung aller Systeme

b) Wiederherstellbarkeit

Es sind folgende Maßnahmen umgesetzt, um zu gewährleisten, dass personenbezogene Daten rasch wiederhergestellt werden können:

- Redundante Infrastruktur
- Regelmäßige Backups
- Regelmäßige und verschlüsselte Backups der Kundendaten
- Backup-Storage an gesondertem Standort
- Regelmäßige Prüfung der Backups auf Verfügbarkeit, Vollständigkeit und Integrität

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

gemäß Art. 32 Abs. 1 lit. d DSGVO und Art. 25 Abs. 1 DSGVO

a) Datenschutzmanagement

- Bestellter Datenschutzbeauftragter
- Sicherheitszertifizierungen nach ISO 27001
- Verwendung von Software-Lösungen für Datenschutz-Management
- Regelmäßige Schulungen der Mitarbeiter sowie Verpflichtung aller Mitarbeiter auf Vertraulichkeit
- Datenschutzfreundliche Voreinstellungen
- Datenschutzzertifizierungen für ausgewählte Produkte der EQS Group AG
- Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen, u.a. durch regelmäßige Audits
- Unternehmensrichtlinien zum Datenschutz
- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung
- Bei Bedarf Durchführung von Datenschutzfolgenabschätzung nach Art. 35 EU-DSGVO
- Dokumentiertes Sicherheitskonzept
- Dokumentierte Prozesse zum Umgang mit Datenschutzvorfällen sowie mit Anfragen Betroffener

b) Incident-Response-Management

- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen
- Intrusion Detection System (IDS)
- Antiviren-Software
- Firewalls
- Dokumentation von Sicherheitsvorfällen und Datenpannen im Rahmen des Informationssicherheitsmanagementsystems
- Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

c) Informationssicherheitsmanagementsystem

- Interner Informationssicherheitsbeauftragter (CISO)
  E-Mail-Adresse: infosec@eqs.com
- Sicherheitszertifizierungen nach ISO 27001
- Regelmäßige Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen
- Informationssicherheitsmanagementsystem (ISMS)

d) Auftragskontrolle

- Sorgfältige Auswahl und Überwachung von Subunternehmern unter Informationssicherheitsgesichtspunkten
- Abgeschlossener Auftragsverarbeitungsvertrag
- Regelmäßige Kontrolle der Vertragsausführung
- Vernichtung von Daten nach Beendigung des Auftrags
- Regelung zum Einsatz weiterer Subunternehmer