Anlage Auftragsdatenverarbeitung EQS Cloud Services (gemäß Art 28 DS-GVO)

Diese Anlage findet Anwendung und konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Vertrag in ihren Einzelheiten beschriebenen Auftragsdatenverarbeitung von personenbezogenen Daten ergeben.

1. Gegenstand und Dauer des Auftrags

Die EQS Group verarbeitet personenbezogene Daten im Auftrag des Kunden für die im Vertrag festgelegte Dauer. Der Kunde gilt als der „Verantwortliche" für die personenbezogenen Daten und die EQS Group als die „Auftragsverarbeiterin".

2. Konkretisierung des Auftragsinhalts

2.1. Art und Zweck der vorgesehenen Verarbeitung von personenbezogenen Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch die EQS Group für den Kunden ergeben sich aus dieser Anlage und dem zwischen den Parteien geschlossenen Vertrag.

2.2. Art der personenbezogenen Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

a) Personenstammdaten (natürlicher Personen: Vorname, Nachname, Organisationsdaten)

b) Kommunikationsdaten (z.B. Telefon, E-Mail, Adresse)

c) Für das Produkt EQS Insider Manager zusätzlich Geburtsdatum und ID Nummern

d) Für Hinweisgebersystem: Informationen zu (potentiellen) Straftaten oder Verdachtsmomenten zu Straftaten und sonstige Meldedaten

2.3. Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

a) Kunden

b) Interessenten

c) Abonnenten

d) Ansprechpartner mit Details

e) Für Hinweisgebersystem: Meldende, sonstige involvierte Personen

3. Pflichten der EQS Group

Die EQS Group verpflichtet sich zur Einhaltung folgender Vorgaben:

3.1. Die EQS Group darf die personenbezogenen Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach Weisung des Kunden verarbeiten, einschließlich der in dieser Anlage und dem Vertrag eingeräumten Befugnisse, es sei denn, dass die EQS Group gesetzlich zur Verarbeitung verpflichtet ist.

3.2. Schriftliche Bestellung eines Datenschutzbeauftragten, der unter der E-Mail datenschutz@eqs.com erreicht werden kann.

3.3. Die EQS Group setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.

3.4. Der Kunde und die EQS Group arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

3.5. Die EQS Group informiert den Kunden unverzüglich über Datenschutzverstöße.

3.6. Soweit der Kunde seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung bei EQS Group ausgesetzt ist, hat ihn EQS Group gegen eine zusätzliche Gebühr zu unterstützen.

3.7. Die EQS Group wird angemessene technische und organisatorische Maßnahmen ergreifen, um personenbezogene Daten vor versehentlicher oder unrechtmäßiger Zerstörung oder versehentlichem Verlust, Veränderung, unberechtigter Offenlegung oder Zugriff zu schützen, insbesondere wenn die Verarbeitung die Übertragung personenbezogener Daten über ein Netzwerk beinhaltet, sowie vor allen anderen unrechtmäßigen Formen der Verarbeitung. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es der EQS Group gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Die EQS Group verpflichtet sich, weiterhin nach ISO 27001 zertifiziert zu bleiben.

3.8. Die EQS Group kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um sicherzustellen, dass die Verarbeitung in ihrem Verantwortungsbereich im Einklang mit den Anforderungen der DS-GVO erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

3.9. Die EQS Group verpflichtet sich zur Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Kunden im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

3.10. Der Cloud Service hält die Bestimmungen der DS-GVO bei ordnungsgemäßem Betrieb durch die Nutzer ein.

4. Pflichten des Kunden

4.1. Bei der Verarbeitung personenbezogener Daten ist der Kunde dafür verantwortlich, die Einhaltung aller geltenden Datenschutzgesetze und -vorschriften sicherzustellen. Der Kunde trägt die alleinige Verantwortung für die Richtigkeit, Qualität und Rechtmäßigkeit der personenbezogenen Daten und die Mittel, mit denen der Kunde personenbezogene Daten erworben hat.

4.2. Der Kunde wird Anfragen der EQS Group nach der Verarbeitung der relevanten personenbezogenen Daten innerhalb einer angemessenen Frist beantworten;

4.3. Der Kunde wird die EQS Group unverzüglich und vollständig informieren, wenn er Fehler oder Unregelmäßigkeiten in Bezug auf den Datenschutz und/oder die Verarbeitung personenbezogener Daten feststellt.

5. Auskunftsrecht, Berichtigung, Einschränkung und Löschung von personenbezogenen Daten

5.1. Die EQS Group darf die personenbezogenen Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Kunden berichtigen, löschen oder deren Verarbeitung einschränken. Soweit der Kunde nicht selbst durch die Funktionalität der zur Verfügung gestellten Leistung in der Lage ist, Auskunft über personenbezogene Daten zu geben, diese zu korrigieren, zu ändern, zu sperren oder zu löschen, wie es die Datenschutzgesetze und -vorschriften erfordern, wird die EQS Group (insofern möglich) einer Aufforderung des Kunden nachkommen, ihn bei der Durchführung zu unterstützen, soweit die EQS Group gesetzlich dazu berechtigt ist. Der Kunde trägt alle Kosten, die sich aus der Bereitstellung dieser Unterstützung durch die EQS Group ergeben.

5.2. Soweit eine betroffene Person sich diesbezüglich unmittelbar an die EQS Group wendet, wird die EQS Group dieses Ersuchen unverzüglich an den Kunden weiterleiten.

6. Unterauftragsverhältnisse

6.1. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen.

6.2. Der Kunde stimmt der Verwendung von Unterauftragnehmern durch die EQS Group zu; dies gilt auch für die Beauftragung von verbundenen Unternehmen der EQS Group und von weiteren Unterauftragnehmern durch die verbundenen Unternehmen. Die EQS Group beachtet das Folgende:

a) Die derzeit von der EQS Group beauftragten Unterauftragnehmer können auf der Website https://www.eqs.com/subprocessor/ abgerufen werden.

b) Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers ist zulässig, soweit:

i. Die EQS Group eine solche Auslagerung auf Unterauftragnehmer dem Kunden mindestens 30 Tage (die „Ankündigungsfrist") vorab in Textform oder auf einer Webseite anzeigt und

ii. eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird, die auch eine Vertraulichkeitsklausel enthält.

iii. Neue Unterauftragnehmer zumindest die gleichen Mindestanforderungen an die Sicherheit erfüllen, wie die existierenden Unterauftragnehmer.

c) Für den Fall, dass der Kunde gegen einen neuen Unterauftragnehmer innerhalb der Ankündigungsfrist Einspruch erhebt, wird die EQS Group angemessene Anstrengungen unternehmen,

i. um dem Kunden eine Änderung der betroffenen Leistung zur Verfügung zu stellen oder

ii. eine wirtschaftlich angemessene Änderung der Konfiguration oder Nutzung der betroffenen Leistung durch den Kunden zu empfehlen, um die Verarbeitung personenbezogener Daten durch den abgelehnten Unterauftragnehmer zu vermeiden, ohne den Kunden unangemessen zu belasten.

Wenn die EQS Group nicht in der Lage ist, diese Änderung innerhalb der Ankündigungsfrist, zur Verfügung zu stellen, kann der

Kunde die jeweilige betroffene Leistung schriftlich außerordentlich kündigen, die von der EQS Group ohne die Verwendung des abgelehnten Unterauftragnehmer nicht bereitgestellt werden kann. Etwaige vorausbezahlte Gebühren für den betroffenen Cloud Service werden anteilig für den Zeitraum ab Inkrafttreten der Kündigung zurückerstattet.

6.3. Die EQS Group wird sich in angemessener Weise bemühen, nur Unterauftragnehmer zu beauftragen, die personenbezogene Daten ausschließlich innerhalb der EU, des EWR oder eines Landes, dem die EU-Kommission ein angemessenes Datenschutzniveau bescheinigt hat, speichern und verarbeiten.

6.4. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU, des EWR oder eines Drittstaats mit angemessenem Schutzniveau stellt die EQS Group die Einhaltung der Bestimmungen der DS-GVO sicher.

7. Kontrollrechte des Kunden

7.1. Die EQS Group verpflichtet sich, dem Kunden auf Anforderung die erforderlichen Auskünfte zur Überprüfung der Einhaltung der in dieser Anlage dargelegten Verpflichtungen zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

7.2. Der Nachweis solcher Maßnahmen kann erfolgen durch

a) die Einhaltung genehmigter Verhaltensregeln;

b) die Zertifizierung nach einem Zertifizierungsverfahren;

c) Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

d) eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

7.3. Sollten diese Nachweise nach überzeugender Darlegung durch den Kunden nicht ausreichend sein, hat der Kunde das Recht, im Benehmen mit der EQS Group Überprüfungen des Schutzes personenbezogener Daten relevanten Verfahren durchzuführen oder durch im Einzelfall zu benennende unabhängige Prüfer durchführen zu lassen. Hierfür ist der Abschluss einer angemessenen Verschwiegenheitsvereinbarung Voraussetzung. Für die Ermöglichung und Durchführung von Kontrollen kann die EQS Group einen Vergütungsanspruch geltend machen. Vor Beginn einer solchen Vor-Ort-Prüfung vereinbaren der Kunde und die EQS Group gemeinsam Umfang, Zeitpunkt und Dauer der Prüfung sowie den Erstattungssatz, für den der Kunde verantwortlich ist. Der Kunde informiert die EQS Group unverzüglich über alle während einer Prüfung festgestellten Verstöße.

8. Unterstützung durch die EQS Group

8.1. Auf Verlangen durch den Kunden unterstützt die EQS Group den Kunden bei seiner Einhaltung der Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen.

8.2. Für diese Unterstützungsleistungen kann die EQS Group eine Vergütung beanspruchen. Die EQS Group hat jedoch keinen Anspruch auf eine Vergütung im Zusammenhang mit

- Datenschutzverletzungen durch die EQS Group, und
- Untersuchungen und Inspektionen durch eine zuständige Aufsichtsbehörde

9. Weisungsbefugnis des Kunden

9.1. Mündliche Weisungen bestätigt der Kunde unverzüglich (mind. Textform).

9.2. Die EQS Group hat den Kunden unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen die DS-GVO. Die EQS Group ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Kunden bestätigt oder geändert wird. Für aus bestätigten Weisungen entstehende Schäden jedweder Art haftet der Kunde der EQS Group im Innenverhältnis voll und stellt die EQS Group gegen Ansprüche Dritter auf erste Anforderung frei.

10. Löschung und Rückgabe von personenbezogenen Daten

10.1. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Kunden nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

10.2. Nach Auslaufen oder Beendigung der Cloud Services oder früher nach Aufforderung durch den Kunden – spätestens mit Beendigung des Vertrages – hat die EQS Group sämtliche in ihrem Besitz gelangten Unterlagen und Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Kunden auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten, sofern dem nicht anderslautende gesetzliche Aufbewahrungsfristen entgegenstehen. Sollte der Cloud-Dienst eine Datenexportfunktionalität enthalten, ist der Kunde dafür verantwortlich, seine Daten vor Ablauf des Vertrags zu extrahieren.