**Auftragsverarbeitungsvertrag nach Art 28 DSGVO**

Die Firma

|  |
| --- |
|  |
|  |
|  |
|  |
|  |

**– nachfolgend Kunde genannt –**

beauftragt die Anqa IT-Security GmbH, Edmund-Rumpler-Straße 5, 51149 Köln

**– nachfolgend AQ genannt –**

mit folgender Auftragsverarbeitung:

Der Kunde hat AQ mit der Durchführung von Awarenessmaßnahmen und Schulungsdienstleistungen beauftragt. AQ wird in diesem Rahmen die Mitarbeiter des Kunden im Hinblick auf mögliche IT-Security Risiken sensibilisieren. Hierbei wird AQ auch die personenbezogenen Daten der Mitarbeiter verarbeiten, soweit dies für die jeweils konkret beauftragten Dienstleistungen erforderlich ist.

Dies vorausgeschickt, vereinbaren die Parteien was folgt:

1. Soweit AQ personenbezogene Daten für den Kunden im Auftrag im Sinne von Art. 28 DSGVO verarbeitet, hat der Kunde AQ im Rahmen der Sorgfaltspflichten des Art. 28 Abs. 1 DSGVO, Art. 24 Abs. 1 und Abs. 2 DSGVO als Dienstleister ausgewählt.

2. Sofern in dieser Vereinbarung der Begriff „Datenverarbeitung“ oder „Verarbeitung (von Daten)“ benutzt wird, entspricht dieser Begriff der Definition in Art 4 Nr. 2 DSGVO.

3. Im Rahmen der Durchführung der Awarenessmaßnahmen und Schulungsdienstleistungen können – je nach konkretem Auftrag – folgende personenbezogenen Daten verarbeitet werden:

* Vornamen und Nachnamen,
* Kommunikationsdaten (wie E-Mail-Adresse; IP-Adresse und MAC-Adresse des jeweils zur Kommunikation verwendeten Gerätes; Telefonnummern),
* Projektdaten (Aktenzeichen; sämtliche Details über Projekte, die elektronisch gespeichert werden),
* Adressdaten, wie postalische Anschriften,
* Informationen über Teilnahme an Awarenessmaßnahmen und Schulungsdienstleistungen und den Schulungsfortschritt einzelner Mitarbeiter

Der Kreis der von der Datenverarbeitung Betroffenen umfasst Mitarbeiter und Geschäftsleitung des Kunden.

4. Der Kunde bleibt verantwortliche Stelle gemäß Art. 4 Nr. 7 DSGVO. Die Beurteilung der Zulässigkeit der Datenverarbeitung obliegt allein dem Kunden. Er ist als verantwortliche Stelle insbesondere für die Wahrung der Betroffenenrechte verantwortlich, die ausschließlich gegenüber dem Kunden wahrzunehmen sind. Der Kunde bestätigt, dass er einen betrieblichen Datenschutzbeauftragten bestellt hat, und wird diesen gegenüber AQ schriftlich oder in Textform bekannt geben.

5. Der Kunde hat das Recht, die Einhaltung der gesetzlichen Vorschriften und der hier vereinbarten Bestimmungen jederzeit im erforderlichen Umfang zu kontrollieren und entsprechende Unterlagen **–** insbesondere im Hinblick auf § 32 DSGVO **–** anzufordern. AQ kann den Nachweis von Maßnahmen, die nicht nur den konkreten Auftrag betreffen, durch Vorlage eines Berichts unabhängiger Instanzen oder einer geeigneten Zertifizierung, insbesondere durch nach Art. 42 DSGVO genehmigte Zertifizierungsverfahren, beibringen.

6. Der Kunde hat das Recht, AQ Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Mündliche Weisungen oder Weisungen in Textform (z. B. E-Mail) sind unverzüglich schriftlich zu bestätigen. Des Weiteren kann der Kunde weisungsberechtigte Personen benennen. Für den Fall, dass sich diese ändern, wird der Kunde dies AQ ebenfalls zeitnah mitteilen.

7. Für den Fall, dass eine Informationspflicht gegenüber Betroffenen und oder Behörden nach Art. 33 und Art. 34 DSGVO besteht, ist der Kunde für die Erfüllung dieser Pflichten verantwortlich; soweit erforderlich, wird AQ den Kunden hierbei unterstützen. Zudem unterstützt AQ den Kunden bei der Erfüllung seiner Verpflichtungen nach Art 35. Und Art 36 DSGVO im erforderlichen und angemessenen Maß.

8. AQ verarbeitet die personenbezogenen Daten ausschließlich im Rahmen der mit dem Kunden getroffenen Vereinbarungen. Zweck, Art und Umfang der Datenverarbeitung richten sich ausschließlich nach Weisungen des Kunden. Eine hiervon abweichende Verarbeitung von Daten ist AQ untersagt.

9. Der Kunde ist verpflichtet, Anträge zur Durchsetzung von Betroffenenrechten gemäß Art. 16 bis 20 DSGVO (z. B. Anträge auf Auskunft oder auf Löschung) nachzukommen. AQ wird den Kunden bei der Erfüllung dieser Verpflichtung unterstützen. AQ wird ausschließlich nach Weisung des Kunden Daten berichtigen, löschen und sperren. Sofern ein Betroffener von AQ die Berichtigung oder Löschung seiner Daten verlangen sollte, wird AQ dies dem Kunden mitteilen. AQ ist zur Wahrung des Datengeheimnisses verpflichtet.

10. AQ sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Dabei sichert AQ auch zu, dass die verarbeiteten Daten des Kunden von sonstigen Datenbeständen getrennt werden. Dazu wird AQ die Betriebsabläufe so gestalten, dass die Daten, die im Auftrag des Kunden verarbeitet werden, im jeweils erforderlichen Maße gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind.

11. AQ wird den Kunden unverzüglich darüber informieren, wenn eine von dem Kunden erteilte Weisung nach Auffassung von AQ gegen gesetzliche Regelungen verstößt. Unabhängig davon ist AQ berechtigt, die Durchführung der betreffenden Weisungen auszusetzen, wenn AQ Zweifel an deren Rechtmäßigkeit hat.

12. Sofern AQ Subunternehmer einsetzt, wird AQ mit den Subunternehmern ebenfalls einen Vertrag nach Art 28 DSGVO abschließen, der die personenbezogenen Daten des Kunden in dem gleichen Maß schützt, wie dies in dem vorliegenden Vertrag vorgesehen ist. Zudem wird AQ vorab und regelmäßig während der Vertragsdauer mit dem Subunternehmer kontrollieren, dass dieser die gemäß Art. 32 DSGVO erforderlichen TOMs zum Schutz personenbezogener Daten getroffen hat und das Ergebnis der Kontrolle für den Kunden dokumentieren und ihm auf Anfrage übermitteln. Auf Anfrage teilt AQ die aktuell beauftragten Subunternehmer mit.

13. AQ hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, und Art. 32 DSGVO in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen. Einzelheiten hierzu sind in **Anlage 1** geregelt. AQ wird den Kunden bei der Verpflichtung des Kunden zur Erfüllung von Art. 32 Abs. 1 DSGVO unterstützen, soweit das hier vertragsgegenständliche Verfahren betroffen ist.

14. Die TOMs unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

15. AQ ist verpflichtet nur solche Personen mit der Verarbeitung von personenbezogenen Daten zu beauftragen, die sich zur Vertraulichkeit verpflichtet haben oder einer gesetzlichen Verschwiegenheitsverpflichtung unterliegen.

16. Soweit der Kunden im Zusammenhang mit dem hier vertragsgegenständlichen Verfahren gemäß Art. 35 DSGVO zu einer Datenschutzfolgeabschätzung verpflichtet ist oder gemäß Art. 36 DSGVO zu einer Konsultation einer Datenschutzaufsichtsbehörde, wird AQ den Kunden unterstützen.

17. Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Kunden wird AQ sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Kunden aushändigen oder nach vorheriger Zustimmung datenschutzgerecht vernichten bzw. löschen. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Daten-verarbeitung dienen, sind durch AQ entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

Köln, den \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_, den \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Anqa IT-Security GmbH Kunde