Auftragsverarbeitungsvertrag nach Art 28 DSGVO

Bereich: UTM-Firewall

Die Firma

_____

_____

_____

_____

_____

– nachfolgend Kunde genannt –

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

– nachfolgend AQ genannt –

mit folgender Auftragsverarbeitung:

AQ wird durch die Bestellung der Leistungen mit der Einrichtung und dem Betrieb einer Firewall-Lösung beauftragt. Hierbei wird AQ auch personenbezogene Daten verarbeiten, soweit dies für die jeweils konkret beauftragten Dienstleistungen erforderlich ist. Dieser Auftragsverarbeitungsvertrag (im Folgenden „AVV“) regelt daher die Verantwortlichkeiten zwischen AQ und dem Kunden („AQ“ und „Kunde“ gemeinsam auch „Parteien“).

Dies vorausgeschickt, vereinbaren die Parteien was folgt:

1. Auslegung

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

2. Datenverarbeitung

Im Rahmen der Durchführung der Verpflichtungen aus der beauftragten Dienstleistung können folgende personenbezogenen Daten verarbeitet werden:

2.1 Kategorien der betroffenen Personen

- Geschäftsleitung und Mitarbeiter des Kunden
- E-Mail Empfänger

2.2 Kategorien der betroffenen Daten

- Vornamen und Nachnamen,
- Kommunikationsdaten von Geschäftsleitern und Mitarbeitern des Kunden (wie E-Mail-Adresse; IP-Adresse und MAC-Adresse des jeweils zur Kommunikation verwendeten Gerätes; Telefonnummern),
- Zugangsdaten von Mitarbeitern und Geschäftsleitung des Kunden,
- Inhaltsdaten geblockter E-Mails,

- Geodaten,
- Aufgerufene URL,
- Kontaktdaten,
- Projektdaten (Aktenzeichen; sämtliche Details über Projekte, die elektronisch gespeichert werden),
- Adressdaten, wie postalische Anschriften,

3. Pflichten der Parteien

3.1. AQ verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Kunden, es sei denn, AQ ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem AQ unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
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 dem AQ ebenfalls zeitnah mitteilen.

3.2 Der Kunde ist 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.

3.3 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 Art. 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.

Darüber hinaus ist der Kunde berechtigt, Vor-Ort-Kontrollen bei AQ durchzuführen oder durch einen Dritten durchführen zu lassen, um die Einhaltung der vertraglichen und gesetzlichen Vorgaben zu überprüfen. Der Auftragnehmer verpflichtet sich, den mit der Kontrolle betrauten Personen den erforderlichen Zutritt und Einblick zu den relevanten Daten, Prozessen und Systemen zu ermöglichen, soweit dies zur Durchführung der Kontrolle notwendig ist. AQ wird alle erforderlichen Auskünfte erteilen, Abläufe demonstrieren und Nachweise führen, die zur Durchführung der Kontrolle erforderlich sind.

Kontrollen durch Dritte kann AQ nur verweigern, wenn ein berechtigtes Interesse, wie etwa ein Wettbewerbsverhältnis, vorliegt oder ähnliche gewichtige Gründe bestehen. Kontrollen beim Auftragnehmer müssen ohne vermeidbare Störungen des Geschäftsbetriebs erfolgen. Soweit keine dringlichen, vom Kunden zu dokumentierenden Gründe vorliegen, finden Kontrollen nur nach angemessener Vorankündigung von vierzehn Tagen, zu den Geschäftszeiten des Auftragnehmers sowie nicht häufiger als alle 12 Monate statt.

3.4 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 dem Auftragsverarbeiter untersagt.

3.5 Der Kunde ist verpflichtet, Anträge zur Durchsetzung von Betroffenenrechten gemäß Kapitel 3 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 unverzüglich mitteilen und den Antrag nicht selbst beantworten. AQ ist zur Wahrung des Datengeheimnisses verpflichtet.

3.6 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.

3.7 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.

4. Subunternehmer

4.1 Sofern AQ Subunternehmer einsetzt, wird AQ mit den Subunternehmern 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. AQ stellt sicher, dass der Subunternehmer die Pflichten erfüllt, denen AQ entsprechend diesen Klauseln und gemäß der DSGVO unterliegt.

4.2 AQ besitzt die allgemeine Genehmigung des Kunden für die Beauftragung von Subunternehmer, die in der **Anlage 2** aufgeführt sind. AQ unterrichtet den Kunden mindestens 14 Tage im Voraus ausdrücklich in Textform über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Subunternehmern und räumt dem Kunden ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Subunternehmer(s) Einwände gegen diese Änderungen erheben zu können. AQ stellt dem Kunden die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

4.3 AQ stellt dem Kunden auf dessen Verlangen eine Kopie der Vereinbarung mit dem/den Subunternehmer(n) und etwaiger späterer Änderungen zur Verfügung.

4.4 AQ haftet gegenüber dem Kunden dafür, dass der Subunternehmer seinen Pflichten gemäß dem mit AQ geschlossenen Vertrag nachkommt. AQ benachrichtigt den Kunden, wenn der Subunternehmer seine vertraglichen Pflichten nicht erfüllt

5. Sicherheit

5.1 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.

5.2 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. Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

5.3 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.

5.4 Falls die Verarbeitung personenbezogene Daten gem Art. 9 DSGVO betrifft, wendet AQ spezielle Beschränkungen und/oder zusätzliche Garantien zum Schutz dieser sensiblen Daten an.

6. Datenübermittlung in Drittstaaten

Jede Übermittlung von Daten durch AQ in einen Drittstaat erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Kunden oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem AQ unterliegt, und muss mit Kapitel V der DSGVO im Einklang stehen. Soweit kein Angemessenheitsbeschluss vorliegt, erfolgt eine Datenverarbeitung nur auf Basis von Standardvertragsklauseln gem. Art. 46 DSGVO (s. Durchführungsbeschluss (EU) 2021/914 oder etwaige Nachfolgeregelungen).

7. Unterstützung des Kunden

7.1 Soweit der Kunde 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. Ebenso unterstützt AQ den Kunden soweit erforderlich bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten.

7.2 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. AQ wird den Kunden bei diesen Pflichten unterstützen. Dazu gehört insbesondere die Mitwirkung bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), die Einholung von Informationen, die gemäß Art. 33 Abs. 3 DSGVO in der Meldung anzugeben sind sowie bei der Einhaltung der Pflicht gemäß Art. 34 DSGVO, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen.

7.3 AQ teilt dem Kunden unverzüglich Verletzungen des Schutzes personenbezogener Daten mit, die im Auftrag des Kunden verarbeitet wurden. Dies gilt auch für begründete Verdachtsfälle. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragsverarbeiters vom relevanten Ereignis zu erfolgen.

Die Mitteilung muss mindestens folgende Angaben enthalten:

a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
d. eine Beschreibung der vom Auftragsverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragsverarbeiters oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen. AQ informiert den Kunden unverzüglich über Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

7.4 Die Kosten der Unterstützungsmaßnahmen trägt der Kunde.

8. Laufzeit, Vertragsbeendigung

8.1 Der Vertrag läuft für die Dauer des Auftrags, soweit er nicht nach einer der nachfolgenden Regelungen vorzeitig beendet wird.

8.2 Der Kunde ist berechtigt, den Vertrag zu kündigen, wenn AQ in erheblichem Umfang oder fortdauernd gegen Regelungen in dieser Vereinbarung verstößt. AQ ist berechtigt, den Vertrag zu kündigen, wenn der Kunde auf der Erfüllung seiner Anweisungen besteht, nachdem er vom AQ darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen verstoßen

8.3 Bei Vertragsbeendigung 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.

9. Haftung

Die Parteien unterstützen sich im Falle einer Inanspruchnahme wechselseitig. Jede Partei haftet im Innenverhältnis gegenüber der anderen nach den Vorgaben des Art. 82 DSGVO.

10. Schlussbestimmungen

10.1 Für die Rechtsbeziehungen zwischen AQ und dem Kunden gilt das Recht der Bundesrepublik Deutschland.

10.2 Ausschließlicher Gerichtsstand für alle Ansprüche und Streitigkeiten aus und im Zusammenhang mit dem Vertragsverhältnis ist Köln. AQ ist jedoch alternativ berechtigt, Klage am allgemeinen Gerichtsstand des Kunden zu erheben.

10.3 Sollten eine oder mehrere der Bestimmungen dieses Vertrags unwirksam oder undurchführbar sein oder werden, wird die Wirksamkeit der übrigen Bestimmungen und des Vertrags, in den sie einbezogen sind, davon nicht berührt. Die Parteien verpflichten sich, die ungültige oder undurchführbare Bestimmung in diesem Fall durch eine wirksame und durchführbare Regelung zu ersetzen, die dem wirtschaftlichen Sinn und Zweck der unwirksamen oder undurchführbaren Bestimmung möglichst nahekommt. Gleiches gilt im Falle einer Regelungslücke

Anlage 1: TOMs
Anlage 2: Liste der Subunternehmer

_____, den_____ _____, den _____

_____ _____
Systemhaus Kunde