**Auftragsverarbeitungsvertrag nach Art 28 DSGVO**

Die Firma

**[einsetzen]**

**– nachfolgend Kunde genannt –**

beauftragt die

**[Vertriebspartner]**

**– nachfolgend Vertriebspartner genannt –**

mit folgender Auftragsverarbeitung (Subunternehmer: Anqa IT-Security GmbH):

Die Parteien haben einen Vertrag über die Erbringung von Service-Supportleistungen („**Service-Vertrag**“) geschlossen. Der Vertriebspartner stellt dabei dem Kunden über die Network Box ein Sicherheitssystem zur Verfügung, mit dem die kundeneigene IT-Infrastruktur von unberechtigten Zugriffen Dritter bestmöglich geschützt wird. Gleichzeitig kann der Kunde über die Network Box auch eigenen Traffic kontrollieren.

Dies vorausgeschickt, vereinbaren die Parteien was folgt:

1. Soweit der Vertriebspartner personenbezogene Daten für den Kunden im Auftrag im Sinne von Art. 28 DSGVO verarbeitet, hat der Kunde den Vertriebspartner 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 des Service-Vertrages wird eine Reihe von Daten des Kunden automatisch auf die Server der von Anqa übertragen. Zudem kann Anqa im Rahmen der Untersuchung von Incidents auch Zugriff auf weitere Daten in den Systemen des Kunden erlangen. Bei vielen dieser Daten handelt es sich um personenbezogene Daten, also um Informationen, die einer natürlichen Person zugeordnet werden können. Hierzu zählen insbesondere folgende Daten, die sich auf Mitarbeiter und Endkunden beziehen können:

● 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,

● weitere personenbezogenen Daten.

Der betroffene Kreis der Personengruppen umfasst die 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 dem Vertriebspartner 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. Der Vertriebspartner 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, dem Vertriebspartner 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 Vertriebspartner 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 der Vertriebspartner den Kunden hierbei unterstützen.

8. Der Vertriebspartner 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 Vertriebspartner 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. Der Vertriebspartner wird den Kunden bei der Erfüllung dieser Verpflichtung unterstützen. Der Vertriebspartner wird ausschließlich nach Weisung des Kunden Daten berichtigen, löschen und sperren. Sofern ein Betroffener vom Vertriebspartner die Berichtigung oder Löschung seiner Daten verlangen sollte, wird der Vertriebspartner dies dem Kunden mitteilen. Der Vertriebspartner ist zur Wahrung des Datengeheimnisses verpflichtet.

10. Der Vertriebspartner sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Dabei sichert der Vertriebspartner auch zu, dass die verarbeiteten Daten des Kunden von sonstigen Datenbeständen getrennt werden. Dazu wird der Vertriebspartner 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. Der Vertriebspartner wird den Kunden unverzüglich darüber informieren, wenn eine von dem Kunden erteilte Weisung nach Auffassung des Vertriebspartners gegen gesetzliche Regelungen verstößt. Unabhängig davon ist der Vertriebspartner berechtigt, die Durchführung der betreffenden Weisungen auszusetzen, wenn der Vertriebspartner Zweifel an deren Rechtmäßigkeit hat.

12. Der Vertriebspartner 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. Der Vertriebspartner wird den Kunden bei der Verpflichtung des Kunden zu der Erfüllung von Art. 32 Abs. 1 DSGVO unterstützen, soweit das hier vertragsgegenständliche Verfahren betroffen ist.

13. Sofern der Vertriebspartner Subunternehmer einsetzt, wird der Vertriebspartner 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.

Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer, welche in Anlage 2 aufgeführt wurden, zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zu.

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. Der Vertriebspartner 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 der Vertriebspartner den Kunden unterstützen.

17. Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Kunden wird der Vertriebspartner 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 Datenverarbeitung dienen, sind durch den Vertriebspartner entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

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

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

Vertriebspartner Kunde