Allgemeine Geschäftsbedingungen

der nicos AG

für die Erbringung von cyber defense Services

Version 1.2

Stand: 09.12.2020

1. Vertragsgegenstand und Geltungsumfang

1.1 **Parteien.** Diese Allgemeinen Geschäftsbedingungen („AGB“) gelten zwischen der nicos AG, Münsterstr. 111, 48155 Münster („wir“, „uns“, oder „unser“) und der vertragsschließenden natürlichen oder juristischen Person („Sie“ oder „Ihr“), die in der jeweiligen Auftragsbestätigung angegeben ist.

1.2 **Vertrag**. Diese AGB gelten für alle Verträge über die Erbringung bestimmter cyber defense Dienstleistungen im Bereich *managed cyber security services* (Detektion, Reaktion, Prävention) einschließlich einer etwaigen Bereitstellung von Hardware und Software auf Grundlage Ihrer von uns durch eine Auftragsbestätigung bestätigten Bestellungen. Die vorgenannten Leistungen werden im Folgenden zusammengefasst als ***Services*** bezeichnet. Die Bestimmungen dieser AGB gemeinsam mit der jeweiligen Auftragsbestätigung werden zusammen als ***Vertrag*** bezeichnet. Mit einer Bestellung bei uns erkennen Sie die AGB in der im Zeitpunkt der Bestellung gültigen Fassung an.

1.3 **Definitionen**. Bestimmte Begriffe, die in diesen AGB verwendet werden, werden in Ziffer 14 oder an anderer Stelle in diesen AGB definiert.

1.4 **Vertragsschluss**. Wir sind erst dann verpflichtet, gegenüber Ihnen die in einer Bestellung beauftragten Services zu erbringen, wenn wir Ihre Bestellung mittels einer Auftragsbestätigung bestätigt haben.

1.5 **Ausschluss**. Nicht von den Services umfasst sind: (i) die Bereitstellung von Hardware, Software und Dienstleistungen, die nach diesem Vertrag nicht ausdrücklich von uns zur Verfügung zu stellen sind und (ii) die Übertragung der Daten von und zu unserer Hardware, insbesondere unseren Servern. Sie sind dafür verantwortlich, eine Internetverbindung und eine geeignete Konnektivität zu den Services auf eigene Kosten sicherzustellen und aufrechtzuerhalten.

2. Bereitstellung von Services

2.1 **Servicestandards**. Wir erbringen die Services im Wesentlichen gemäß unserer Produktbeschreibung wie in der Auftragsbestätigung aufgeführt. Die Inanspruchnahme unserer Services garantiert Ihnen nicht, dass Sie vor Cyber-Security-Angriffen oder -Vorfällen sicher sind, dass wir die Herkunft von Cyber-Security-Angriffen identifizieren können und dass wir von einem Cyber-Security-Vorfall betroffene Systeme und/oder Daten wieder herstellen.

2.2 **Reports.** Von uns zur Verfügung gestellte Reports sind jeweils auf eine Cyber-Security Analyse eines bestimmten Teils Ihrer IT-Systeme, zu einem bestimmten Zeitpunkt und im Hinblick auf spezifisch getestete, mögliche IT-Sicherheitsschwachstellen beschränkt. Die Reports stellen keine umfassende Dokumentation Ihrer IT-Sicherheit dar.

2.3 **Sicherheit**. Wir verfügen über ein Sicherheitsprogramm, das entwickelt wurde, um Ihre Inhalte vor Sicherheitsgefährdungen und -bedrohungen zu schützen und

den unberechtigten Zugriff auf Ihre Inhalte zu verhindern. Unsere Cloud-Infrastruktur basiert auf einem Sicherheitsprogramm, das u.a. den Anforderungen von ISO 27001 oder einem etwaigen Nachfolge-Standard der ISO 27001 im Wesentlichen entspricht und der zumindest das gleiche Schutzniveau bietet, das durch die ISO 27001-Zertifizierung des Lieferanten dokumentiert wird. Dieser Abschnitt regelt unsere Verpflichtungen in Bezug auf die Sicherheit der Services und Ihrer Inhalte abschließend.

2.4 **Änderungen der Services**. Während laufender Bestellzeiträume dürfen wir die Funktionsfähigkeit unserer Services nur aus folgenden Gründen einschränken oder beenden, nachdem wir Sie mit angemessener Vorlaufzeit – soweit möglich – darüber informiert haben: (i) rechtliche Anforderungen; (ii) durch unsere Subdienstleister verursachte Änderungen bei den Leistungen; (iii) die Beendigung der Zusammenarbeit mit einem Lieferanten von Software, Hardware und/oder Dienstleistungen, die für die Erbringung der Leistungen wesentlich sind; und/oder (iv) Sicherheitsrisiken. Im Fall einer Beschränkung können Sie die betroffene Leistung bis 30 Tage vor dem von uns angekündigten Datum des Inkrafttretens der Einschränkung kündigen. Im Falle einer solchen Kündigung oder Beendigung einer Leistung werden wir Ihnen einen etwaigen für die betreffende Leistung vorausbezahlten Betrag anteilig erstatten. Bis zu 8 Wochen vor dem Zeitpunkt der Verlängerung eines Bestellzeitraums (Ziffer 10.1) können wir Ihnen eine Auftragsbestätigung mit geänderten Konditionen schicken. Diese gilt für den verlängerten Bestellzeitraum. Sollten Sie die Services zu den geänderten Konditionen nicht beziehen wollen, können Sie die von den Änderungen betroffenen Services innerhalb von 30 Tagen nach Zugang der Auftragsbestätigung mit Wirkung zum Ende des laufenden Bestellzeitraums kündigen.

2.5 **Änderungen dieser AGB.** Die zum Datum der Auftragsbestätigung geltenden AGB gelten bis zum Ende des Bestellzeitraums, einschließlich etwaiger Verlängerungszeiträume gemäß Ziffer 10.1, für die mit dieser Auftragsbestätigung bestellten Services, es sei denn, eine Änderung während des Bestellzeitraums ist durch eine Änderung der Rechtslage erforderlich oder nach den Regelungen dieses Vertrags erlaubt. Sollte eine Änderung während des Bestellzeitraums eine wesentliche nachteilige Auswirkung auf die Nutzung der Services haben, können Sie den von der Änderung betroffenen Service innerhalb von 30 Tagen nach Mitteilung der Änderung durch uns kündigen. In einem solchen Fall werden wir Ihnen den für den jeweiligen Service vorausbezahlten Betrag anteilig erstatten.

2.6 **Subdienstleister.** Für die Erbringung der Services nutzen wir Subdienstleister. Soweit in unseren Produkt- oder Leistungsbeschreibungen der jeweilige Subdienstleister als Leistungserbringer der Services benannt ist, kommt, vorbehaltlich ausdrücklicher abweichender Vereinbarungen, kein Vertrag zwischen diesem Subdienstleister und Ihnen zustande. Eine Vertragsbeziehung besteht insofern nur zwischen Ihnen und uns.

2.7 **Datenschutz.** Soweit wir bei der Erbringung der Services personenbezogene Daten verarbeiten, die sich auf Ihren IT-Systemen einschließlich Ihrer Netzwerkverbindung befinden, sind wir für den jeweiligen Bestellzeitraum als Auftragsverarbeiter für Sie tätig. Insoweit finden die Bestimmungen der Vereinbarung zur Auftragsverarbeitung (**Anlage 1**) Anwendung.

3. Mitwirkungspflichten

3.1 **Zurverfügungstellung von Informationen; Unterstützung.** Sie stellen uns die für die Erbringung der Services notwendigen Informationen, Daten und Unterlagen, einschließlich der in der Leistungsbeschreibung aufgeführten, rechtzeitig und jedenfalls vor Beginn der Erbringung der Services zur Verfügung. Ferner gewähren Sie die von uns erbetene angemessene Unterstützung zur Erbringung der Services.

3.2 **Zugang.** Sie gewähren uns und unseren Subdienstleistern, soweit erforderlich, Zutritt zu den Räumlichkeiten, in denen die Services erbracht werden sollen.

3.3 **Sicherheit.** Soweit wir oder unsere Subdienstleister die Services in Ihren oder anderen von Ihnen bestimmten Räumlichkeiten erbringen, stellen Sie, soweit möglich, die Sicherheit der entsprechenden Mitarbeiter sicher. Sie informieren uns im Voraus über etwaige Risiken oder Gefahren.

3.4 **Fehlende Erbringung der Unterstützungsleistungen.** Soweit wir unsere Leistungen nicht erbringen können, weil Sie die vorgenannten Unterstützungsleistungen nicht erbringen, verletzen wir unsere vertraglichen Verpflichtungen nicht und Sie sind zur Zahlung der vereinbarten Vergütung verpflichtet.

4. Hardwaremiete

4.1 **Bestimmungsgemäßer Einsatz und Lieferkosten.** Gemietete Hardware werden Sie nur bestimmungsgemäß und im Rahmen unserer Instruktionen einsetzen, ordnungsgemäß behandeln, vor unbefugtem Zugriff sichern und schützen und nach Ablauf der Miete zurückgeben. Sie tragen die Kosten für Verpackung, Hin- und Rückversand oder sonstige Lieferung der gemieteten Hardware.

4.2 **Meldepflicht.** Defekte und/oder den Verlust der gemieteten Hardware werden Sie uns unverzüglich melden. Wir werden uns bemühen, defekte Hardware innerhalb von 7 Kalendertagen nach Zugang dieser Meldung auszutauschen.

4.3 **Besichtigung und Untersuchung.** Wir dürfen die gemietete Hardware während Ihrer üblichen Betriebszeiten nach angemessener Vorankündigung besichtigen und untersuchen bzw. durch einen Beauftragten untersuchen lassen.

4.4 **Rechte Dritter.** Für den Fall, dass Dritte Rechte an gemieteter Hardware Ihnen gegenüber geltend machen, sind Sie verpflichtet, uns unverzüglich davon zu unterrichten und den Dritten über das bestehende Mietverhältnis in Kenntnis zu setzen.

5. Vergütung, Zahlungsbedingungen und Steuern

5.1 **Allgemein.** Die Vergütung für die Services ergibt sich aus der Auftragsbestätigung. Die Vergütung ist bei Erhalt der Rechnung fällig und innerhalb von 30 Tagen ab Rechnungsdatum unter Verwendung einer der von uns unterstützten Zahlungsmethoden ohne Abzüge und ohne dass zusätzliche Kosten für uns anfallen zahlbar. Auf verspätete Zahlungen erheben wir den jeweiligen gesetzlichen Verzugszinssatz.

5.2 **Vergütung nach Aufwand.** Sofern wir unsere Services oder Teile unserer Services auf Zeit- und Materialbasis (Aufwand) erbringen, so geben wir auf Verlangen eine unverbindliche Kostenschätzung; maßgeblich bleibt der tatsächlich benötigte Zeitaufwand, falls nicht etwas anderes ausdrücklich in Textform vereinbart wird.

5.3 **Erhöhung der Vergütung.** Soweit sich der Bestellzeitraum für einen oder mehrere Services gemäß Ziffer 10.1 verlängert und in der Auftragsbestätigung nichts Abweichendes geregelt ist, sind wir berechtigt, die Vergütung für den jeweiligen Verlängerungszeitraum nach billigem Ermessen marktkonform zu erhöhen. Eine solche Erhöhung wird 30 Tage nach Zugang einer entsprechenden Mitteilung wirksam, frühestens jedoch mit Beginn des Verlängerungszeitraums. In diesem Fall können Sie den von der Erhöhung betroffenen Service innerhalb von 30 Tagen nach Zugang der Mitteilung der Erhöhung kündigen, frühestens jedoch mit Wirkung zu Beginn des von der Erhöhung betroffenen Verlängerungszeitraums.

5.4 **Steuern.** Alle Preise verstehen sich exklusive Steuern, Zöllen und Einfuhrabgaben sowie sonstiger Gebühren. Jegliche anfallende Steuern, Zölle, Einfuhrabgaben und sonstigen Gebühren sind von Ihnen zu übernehmen. Sollten Steuern, Zölle oder Abgaben, die von Ihnen zu tragen sind, auf fällige Zahlungen an uns erhoben oder einbehalten werden, so sind Ihre Zahlungen an uns um den Betrag zu erhöhen, der erforderlich ist, damit wir den gleichen Betrag erhalten, wie wenn solche Steuern, Zölle oder Abgaben nicht einbehalten worden wären. In jedem Fall sind Sie verpflichtet, uns umgehend das offizielle Dokument zur Verfügung zu stellen, das die Steuerzahlung in Ihrem Namen bestätigt.

6. Rechte

6.1 **Rechte an Ihren Inhalten.** Wir erwerben keine Rechte oder Ansprüche bezüglich Ihrer Inhalte, sofern diese nicht in diesem Vertrag geregelt sind. Wir und unsere Subdienstleister haben das weltweite, nicht exklusive, übertragbare, unterlizenzierbare und vergütungsfreie Recht, Ihre Inhalte, soweit dies für die Zwecke der Erbringung der Services erforderlich ist, zu nutzen.

6.2 **Rechte an den Services, Reports, Feedback.** Alle Rechte, Eigentum und Ansprüche bezüglich der Services, einschließlich Dokumentationen und Reports, auch Teilen hiervon, sowie Verbesserungen, einschließlich sämtlichen Know-hows sowie alle diesbezüglichen geistigen Eigentumsrechte verbleiben

vollständig bei uns oder unseren Geschäftspartnern und/oder deren Lizenzgebern. Wir räumen Ihnen das nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, zeitlich beschränkte und widerrufliche Recht zur Nutzung unserer Services ein, soweit dies für die bestimmungsgemäße Nutzung der Services nach Maßgabe dieses Vertrages erforderlich ist. Sie räumen uns ein weltweites, unbefristetes, unwiderrufliches, unbeschränktes, übertragbares, unterlizenzierbares, vergütungsfreies Recht ein, alle Anregungen, Empfehlungen, Funktionalitätsanfragen oder sonstiges Feedback im Zusammenhang mit den Services, die von Ihnen oder in Ihrem Auftrag übermittelt werden, zu verwenden.

7. Gewährleistung

Wir gewährleisten, dass die Services in Übereinstimmung mit den Regelungen in Ziffer 2.1 erbracht werden. Sollten Services nicht wie zugesagt erbracht werden, sind unsere Verpflichtungen, soweit rechtlich zulässig, darauf beschränkt: (i) wirtschaftlich zumutbare Bemühungen zu unternehmen, um den betroffenen Service so wiederherzustellen, dass er gemäß Ziffer 2.1 erbracht wird, oder (ii) falls eine solche Wiederherstellung nach unserer Einschätzung nicht innerhalb eines angemessenen Zeitrahmens oder mit vertretbarem wirtschaftlichem Aufwand zu erreichen ist, den betroffenen Service einzustellen und etwaige im Voraus gezahlte Beträge für diesen Service für den verbleibenden Bestellzeitraum anteilig zu erstatten. Sie sind verpflichtet, uns etwaige Mängel der Services unverzüglich zu melden.

8. Haftungsbeschränkung

8.1 **Haftungsbegrenzung.** Unsere Haftung ist für alle Ansprüche, Schadensersatzforderungen und Entschädigungen, die aus oder im Zusammenhang mit dem Vertrag entstehen, unabhängig von der Art des Anspruchs, wegen Vertragsverstößen, aus unerlaubten Handlungen oder aus sonstigen Gründen, beschränkt auf die Summe der von Ihnen an uns während der 12 Monate vor Entstehen der Forderung gezahlten Vergütung für den Service, der Gegenstand des Anspruchs ist.

8.2 **Haftungsausschluss.** Wir haften nicht für Produktionsverluste, Betriebsunterbrechungen, vertragliche Ansprüche von Dritten gegen Sie, Vermögensschäden, Verluste oder Beschädigung Ihrer Inhalte, Nutzungsausfälle, Zinsverluste, entgangene Einnahmen, Gewinne oder Ersparnisse oder indirekte Schäden, Nebenschäden, Folgeschäden, Strafgelder oder sonstige Schadensersatzansprüche. Dies gilt auch dann, wenn wir über die Möglichkeit solcher Schäden im Voraus informiert wurden.

8.3 **Geltendmachung von Ansprüchen.** Alle Ansprüche gegen uns müssen spätestens innerhalb von 12 Monaten nach dem Ereignis, dem der jeweilige Anspruch zugrunde liegt, geltend gemacht werden. Nach Ablauf dieser Frist sind Ansprüche gegen uns aufgrund dieses Ereignisses ausgeschlossen.

8.4 **Umfang der Haftungsbegrenzung, -beschränkung und des Haftungsausschlusses.** Die Haftungsbegrenzungen, -beschränkungen und Haftungsausschlüsse in dieser Ziffer 8.1 - 8.3 gelten nicht (i) für vertragliche Verpflichtungen, deren Erbringung wesentlich für die ordnungsgemäße Erfüllung des Vertrags ist (*Kardinalpflichten*), wobei unsere Haftung insoweit auf typische und voraussehbare Schäden oder Verluste beschränkt ist; (ii) in Fällen von Vorsatz oder grober Fahrlässigkeit; (iii) in Fällen von Körper- oder Gesundheitsschäden oder Todesfällen, die wir oder unsere gesetzlichen Vertreter oder unsere Subdienstleister fahrlässig verursachen; (iv) in Fällen von Betrug oder arglistiger Täuschung; und (v) in dem Umfang, in dem die Haftung nach Produkthaftungsrecht nicht eingeschränkt oder ausgeschlossen werden kann.

8.5 **Begünstigte.** Die Regelungen dieser Ziffer 8 gelten auch für alle Arbeitnehmer, Vorstandsmitglieder, Geschäftsleiter, Vertreter, Lieferanten, Subdienstleister und alle sonstigen Personen, die für uns bei der Erfüllung unserer Verpflichtungen tätig werden.

9. Zurückbehaltung von Services

9.1 **Unser Recht auf Zurückbehaltung von Services.** Wir dürfen unsere Services sperren oder einschränken, falls wir vernünftigerweise davon ausgehen dürfen, dass Sie gegen Ihre Verpflichtungen nach diesem Vertrag verstoßen oder falls eine solche Sperrung oder Einschränkung durch Gesetze, in Folge einer Gerichtsentscheidung oder einer Aufforderung einer staatlichen Behörde erforderlich wird. Zudem sind wir berechtigt, Rechenvorgänge zu verlangsamen oder zu beenden, wenn wir der Meinung sind, dass diese die Erbringung der Services ganz oder teilweise beeinträchtigen.

9.2 **Auswirkungen einer Zurückbehaltung von Services.** Ihre Verpflichtung zur Zahlung der Vergütung bleibt unberührt. Die Sperrung oder Einschränkung wird aufgehoben, sobald der Grund hierfür nicht länger besteht. Unser Recht zur Kündigung nach Ziffer 10 und unsere sonstigen Rechte bleiben unberührt.

10. Laufzeit, Kündigung

10.1 **Bestellzeitraum.** Der Bestellzeitraum einer Bestellung beträgt 36 Monate ab dem Zugang der Auftragsbestätigung (Ziffer 1.4), soweit nicht anders in der Auftragsbestätigung festgelegt. Während eines Bestellzeitraums kann ein Service nicht ordentlich gekündigt werden. Soweit nicht anders in der Auftragsbestätigung festgelegt, verlängert sich der Bestellzeitraum um jeweils weitere 12 Monate, sofern nicht eine Partei spätestens 6 Monate vor Ablauf des jeweiligen Bestellzeitraums den betreffenden Service kündigt. Das Kündigungsrecht gemäß Ziffer 2.4 bleibt unberührt.

10.2 **Kündigung aus wichtigem Grund.** Das Recht zur Kündigung von Services aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund liegt insbesondere vor bei einem wesentlichen Vertragsverstoß der anderen Partei, wenn dieser Verstoß nicht innerhalb von 30 Tagen ab dem Zugang einer Information durch die

andere Partei über den Verstoß behoben wird oder wenn der Verstoß unbehebbar ist. Insbesondere berechtigen uns die Nichtzahlung der Vergütung innerhalb von 15 Tagen nach dem Erhalt einer Mahnung oder Verletzungen von Ziffern 3 oder 12 zur Kündigung aus wichtigem Grund. Das Recht zur Kündigung beschränkt sich auf den von dem Vertragsverstoß betroffenen Service.

10.3 **Folgen der Beendigung eines Services.** Mit Ablauf des Bestellzeitraums beziehungsweise mit Wirksamwerden der Kündigung eines Services sind wir nicht verpflichtet, diesen Service Ihnen gegenüber weiter zu erbringen und Sie müssen, unabhängig von dem Grund der Kündigung, sofort: (i) die Nutzung der betroffenen Services einstellen; und (ii) alle Materialien (einschließlich Software und Hardware), die im Zusammenhang mit den gekündigten Services stehen, an uns zurückgeben oder auf unsere Anweisung hin zerstören. Sofern nicht abweichend in diesen AGB festgelegt, müssen Sie uns die vollständige Vergütung zahlen, die zum Zeitpunkt der Kündigung fällig war. Wenn Sie aus wichtigem Grund gemäß Ziffer 10.2 kündigen und eine Vorauszahlung geleistet haben, werden wir Ihnen für den nach der Kündigung verbleibenden Bestellzeitraum einen angemessenen Teil der Vorauszahlung erstatten. Die Regelungen der Ziffer 11 gelten fort.

11. Vertraulichkeitsregelungen

11.1 **Geheimhaltungspflichten.** Jede Partei ist verpflichtet, von der anderen Partei oder ihren Verbundenen Unternehmen offengelegte Vertrauliche Informationen vertraulich zu behandeln, sie nur im Zusammenhang mit den Services und wie im Vertrag gestattet zu verwenden und solche Vertraulichen Informationen niemandem offenzulegen außer denjenigen Nutzern, Arbeitnehmern, Verbundenen Unternehmen, Geschäftspartnern und Beratern und den jeweiligen Arbeitnehmern, Geschäftspartnern und Beratern solcher Verbundenen Unternehmen, die für die Erfüllung des Vertrages Kenntnis von diesen Informationen haben müssen und Vertraulichkeitspflichten unterliegen, die zumindest denjenigen dieses Vertrages entsprechen.

11.2 **Offenlegungspflicht.** Wir werden Vertrauliche Informationen und/oder Ihre Inhalte nicht gegenüber Dritten offenlegen, es sei denn (i) Sie weisen uns diesbezüglich an, (ii) dies ist nach dem Vertrag zulässig, oder (iii) wir sind hierzu durch Gesetze oder eine behördliche Anordnung verpflichtet. Sollte ein Dritter (einschließlich öffentlicher Stellen) Kontakt mit uns aufnehmen und von uns verlangen, Vertrauliche Informationen und/oder Ihre Inhalte offenzulegen, werden wir diesen Dritten zunächst darauf verweisen, diese Daten unmittelbar bei Ihnen anzufordern und ihm Ihre Kontaktdaten übermitteln, soweit dies nicht durch Gesetze oder behördliche Anordnung ausgeschlossen ist. Sollten wir gezwungen werden, Vertrauliche Informationen und/oder Ihre Inhalte einem Dritten gegenüber offenzulegen, werden wir Sie sofort darüber informieren und Ihnen eine Kopie der Anordnung übermitteln, soweit dies nicht durch Gesetze oder behördliche Anordnung ausgeschlossen ist. Darüber hinaus können wir Vertrauliche Informationen und/oder Ihre Inhalte Dritten gegenüber offenlegen,

um diese über mögliche Verstöße gegen Gesetze im Zusammenhang mit Ihrer Nutzung der Services zu unterrichten.

12. Exportkontrolle und Sanktionen

12.1 **Einhaltung von Exportkontrollvorgaben.** Die Services und die damit verbundene Zurverfügungstellung von Hardware und/oder Software (zusammen ***Kontrollierte Technologie***) können Exportkontrollen und Sanktionen unterliegen. Sie verpflichten sich zur Einhaltung aller einschlägigen Exportkontrollen und Sanktionen und sichern zu, keine Kontrollierte Technologie (i) ohne entsprechende Genehmigung (soweit notwendig), (ii) an Sanktionierte Personen oder (iii) auf andere gegen Exportkontrollen und Sanktionen verstoßende Art zu exportieren, reexportieren oder übertragen.

12.2 **Keine Sanktionierte Person.** Sie sichern zu, dass weder Sie selbst noch eine Ihrer Tochtergesellschaften oder einer Ihrer Geschäftsführer oder leitenden Angestellten (i) eine Sanktionierte Person ist; und (ii) an Transaktionen, Aktivitäten oder Verhaltensweisen beteiligt war oder ist, die für uns einen Verstoß oder eine Nichteinhaltung von Exportkontrollen und Sanktionen darstellen würden.

12.3 **Recht zur Leistungsverweigerung.** Wir sind nicht zur Erbringung unserer Services verpflichtet, wenn dies durch Exportkontrollen und Sanktionen verhindert wird bzw. zu einem Verstoß gegen Exportkontrollen und Sanktionen führen würde.

12.4 **Kündigungsrecht.** Wir haben das Recht, diesen Vertrag mit sofortiger Wirkung zu kündigen, wenn (i) Sie eine Sanktionierte Person werden, (ii) wir Kenntnis davon erlangen, dass Sie Kontrollierte Technologie unter Verletzung von Exportkontrollen und Sanktionen verwenden oder (iii) wir durch das Festhalten am Vertrag Exportkontrollen und Sanktionen verletzen würden.

13. Allgemeine Bestimmungen

13.1 **Übertragung.** Wir sind berechtigt, den Vertrag, die darin gewährten Rechte sowie die Durchführung einzelner Bestellungen an Dritte zu übertragen. Sie dürfen ohne unser vorheriges, schriftliches Einverständnis weder den Vertrag noch die darin gewährten Rechte vollständig oder teilweise an Dritte übertragen.

13.2 **Aufrechnung, Zurückbehaltungsrecht.** Sie dürfen nur mit solchen Forderungen aufrechnen oder ein Zurückbehaltungsrecht im Zusammenhang mit solchen Forderungen geltend machen, die unbestritten oder von uns anerkannt sind oder die rechtskräftig festgestellt wurden.

13.3 **Höhere Gewalt.** Keine Partei ist für die Nichterfüllung oder verspätete Erfüllung von Verpflichtungen nach dem Vertrag verantwortlich, wenn sich die Gründe hierfür nach vernünftigen Maßstäben der Einflussmöglichkeit dieser Partei entziehen. Hierzu zählen insbesondere Naturereignisse, Erdbeben, Brände, Fluten, Epidemien, Embargos, Aufstände, Sabotage, Angriffe auf unsere IT-Systeme durch Dritte, Arbeitskräftemangel oder Arbeitskämpfe,

Handlungen oder Unterlassungen von Behörden, Krieg, Sabotageakte oder terroristische Anschläge.

13.4 **Anwendbares Recht.** Der Vertrag unterliegt dem Recht der Bundesrepublik Deutschland unter Ausschluss des Kollisionsrechts. Das UN-Kaufrecht findet keine Anwendung.

13.5 **Gerichtsstand.** Gerichtsstand ist Münster, Deutschland.

13.6 **Wirksamkeit und Durchsetzbarkeit.** Sollte eine Bestimmung des Vertrags ungültig, unwirksam oder nicht durchsetzbar sein, wird davon die Gültigkeit, die Rechtmäßigkeit und die Durchsetzbarkeit der übrigen Bestimmungen in keiner Weise berührt. Statt dieser werden die Parteien eine Bestimmung vereinbaren, die anwendbarem Recht und den ursprünglichen Absichten der Parteien so weit wie möglich entspricht.

13.7 **Gesamter Vertrag.** Der Vertrag bildet die Gesamtheit der zwischen den Parteien vereinbarten Vertragsbedingungen in Bezug auf den Vertragsgegenstand ab und ersetzt alle diesbezüglichen vorherigen schriftlichen oder mündlichen Vereinbarungen, Übereinkünfte oder Absprachen. Entgegenstehende Geschäftsbedingungen gelten nicht.

13.8 **Schriftform.** Änderungen, Ergänzungen oder Kürzungen dieses Vertrages bedürfen vorbehaltlich abweichender Regelungen in diesem Vertrag zu ihrer Wirksamkeit der Schriftform. Dies gilt auch für Änderungen dieses Schriftformerfordernisses.

13.9 **Rangfolge.** Im Falle eines Konflikts oder eines Widerspruchs zwischen Regelungen in einzelnen Dokumenten, gelten die Dokumente in der folgenden, absteigenden Reihenfolge: (i) Auftragsbestätigung; (ii) die anwendbaren Produkt- oder Leistungsbeschreibungen; (iii) die Bestimmungen der Vereinbarung zur Auftragsverarbeitung; (iv) diese AGB.

14. Definitionen

14.1 „Auftragsbestätigung“ bezeichnet ein Dokument, ein elektronisches Formular oder ein Online-Instrument, das von uns für Ihre Bestellung von Services bereitgestellt wird.

14.2 „Bestellzeitraum“ bezeichnet den Zeitraum, für welchen in der Auftragsbestätigung die Erbringung eines Services vereinbart wurde.

14.3 „Dritter“ bezeichnet jede natürliche oder juristische Person außer Ihnen oder uns. Dritter umfasst auch Ihre Verbundenen Unternehmen.

14.4 „Exportkontrollen“ und „Sanktionen“ sind Wirtschafts- oder Finanzsanktionen, Handelsembargos, Exportkontrollen oder andere Verbote von Geschäftsaktivitäten, die von den USA, der EU, den Vereinten Nationen, Deutschland oder einem Land, in das Kontrollierte Technologie importiert oder reexportiert wird, verhängt, verwaltet oder durchgesetzt werden.

14.5 „Gemietete Hardware“ bezeichnet Hardware, die Sie – wie in der konkreten Auftragsbestätigung festgelegt – im Zusammenhang mit unserer Erbringung von Services gemietet haben.

14.6 „Gesetze“ bezeichnet jedes Gesetz, jede Vorschrift, Verordnung, Norm und Richtlinie, insbesondere alle branchen- oder unternehmensspezifischen Regelungen, Mitbestimmungsrechte des Betriebsrats, Datenschutz-, Telekommunikations-, und energierechtliche Regelungen, IT-Sicherheitsgesetze, Exportkontrollrecht, Sanktionen und Bestimmungen in Bezug auf den Schutz geheimer Informationen.

14.7 „Ihre Inhalte“ bezeichnet alle Informationen, Programme, Software, Apps, Programmcodes jeglicher Art, Skripte, Bibliotheken oder Daten, die im Zusammenhang mit dem Empfang der Services durch Sie oder in Ihrem Namen an uns übertragen oder weitergegeben werden. Die Services fallen nicht unter Ihre Inhalte.

14.8 „Partei“ bezeichnet Sie und/oder uns, je nach Kontext.

14.9 „Reports“ bezeichnet schriftliche oder digitale Dokumentationen von durch uns im Rahmen der Erbringung von Services durchgeführten Analysen, insbesondere im Hinblick auf die Cyber-Security Ihrer IT-Systeme.

14.10 „Sanktionen“ siehe Exportkontrollen.

14.11 „Sanktionierte Person“ bezeichnet jede Person, (i) die in einer von den USA, der EU, Deutschland, den Vereinten Nationen und dem Vereinigten Königreich herausgegebenen Sanktionsliste aufgeführt ist, (ii) die im Eigentum oder unter der Kontrolle oder im Auftrag einer auf einer solchen Sanktionsliste gelisteten Person steht oder (iii) die auf andere Weise von Sanktionen betroffen ist.

14.12 „Verbundene Unternehmen“ bezeichnet Unternehmen, an denen eine der Parteien mehrheitlich beteiligt ist oder die von einer Partei kontrolliert werden oder die an einer der Parteien mehrheitlich beteiligt sind oder eine der Parteien kontrollieren oder die unter gemeinsamer Kontrolle einer der Parteien stehen, wobei die Beteiligung und Kontrolle jeweils direkt oder indirekt erfolgen kann und „Kontrolle“ die direkte oder indirekte Möglichkeit bezeichnet, die Geschäfte einer anderen Gesellschaft oder juristischen Person zu führen oder über ihre Geschäftspolitik zu entscheiden.

14.13 „Vertrauliche Informationen“ bezeichnet alle Informationen, die von einer Partei oder ihren Verbundenen Unternehmen der anderen Partei gegenüber im Zusammenhang mit dem Vertrag offengelegt werden und die – bei der Offenlegung – als „Vertraulich“ gekennzeichnet werden oder Informationen enthalten, die ihrem Wesen nach oder durch den Kontext, in dem sie mitgeteilt werden, für die empfangende Partei hinreichend deutlich als vertraulich zu erkennen sind. Darüber hinaus gelten alle Informationen und Materialien, die Sie im Zusammenhang mit dem Vertrag oder Ihrer Nutzung der Services erhalten, als Vertrauliche Informationen, insbesondere betreffend die Leistung und

Verfügbarkeit der Services, Reports, Informationen in Bezug auf Geschäftsstrategien und -methoden, Geschäftsgeheimnisse, Know-how, Preisgestaltung, Technologie, Software, APIs, API-Signaturen, Produktpläne, sowie Informationen über Arbeitnehmer, Kunden, Vertriebspartner und Berater von uns. Vertrauliche Informationen umfassen nicht Informationen, die (i) ohne Verletzung des Vertrages und ohne Verletzung rechtlicher Verpflichtungen der Öffentlichkeit allgemein zugänglich sind; (ii) dem Empfänger von einer Quelle übermittelt werden, die eine andere Partei als diejenige ist, die die Vertraulichen Informationen offengelegt hat, vorausgesetzt, dass der Empfänger keinen Grund zu der Annahme hat, dass diese Quelle selbst Vertraulichkeitsverpflichtungen unterliegt oder die Informationen durch unrechtmäßige oder unerlaubte Handlungen erhalten hat; (iii) vor dem Erhalt von der anderen Partei rechtmäßig ohne entsprechende Geheimhaltungsverpflichtung im Besitz des Empfängers waren; (iv) vom Empfänger unabhängig und ohne Nutzung oder Bezugnahme auf Vertrauliche Informationen entwickelt werden.

Anlagen

Anlage 1: Auftragsverarbeitungsvereinbarung

Anlage 2: Unterauftragnehmer

Anlage 3: Technische und organisatorische Maßnahmen der nicos AG

Anlage 1
Auftragsverarbeitungsvereinbarung

Soweit wir bei der Erbringung der Services (Ziffer 1.2 der AGB) personenbezogene Daten verarbeiten, die sich auf Ihren IT-Systemen einschließlich Ihrer Netzwerkverbindung befinden, sind wir für den jeweiligen Bestellzeitraum als Auftragsverarbeiter für Sie tätig. Es finden dann die nachfolgenden Bestimmungen Anwendung. Wir verarbeiten die personenbezogenen Daten für den Zweck der Erbringung der in der Auftragsbestätigung und den zugehörigen Leistungsbeschreibungen aufgeführten Leistungen.

1. Wir verarbeiten die personenbezogenen Daten nur auf Ihre dokumentierte Weisung hin, sofern wir nicht aufgrund gesetzlicher Bestimmungen zur Verarbeitung verpflichtet sind. In diesem Fall teilen wir Ihnen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

2. Wir verpflichten die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit, sofern diese nicht einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

3. Wir ergreifen die als **Anlage 3** beigefügten geeigneten technischen und organisatorischen Maßnahmen zum angemessenen Schutz der zu verarbeitenden personenbezogenen Daten gemäß Artikel 32 Datenschutzgrundverordnung (DSGVO).

4. Wir unterstützen Sie in vernünftigem wirtschaftlich zumutbaren Umfang und unter Berücksichtigung der Art der Verarbeitung mit geeigneten technischen und organisatorischen Maßnahmen dabei, Ihrer Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Artikel 12 bis 23 DSGVO genannten Rechte der betroffenen Person nachzukommen sowie bei Ihrer Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten.

5. Nach Abschluss der Erbringung der Verarbeitungsleistungen löschen wir die im Rahmen der Auftragsverarbeitung verarbeiteten personenbezogenen Daten oder geben sie zurück und löschen die vorhandenen Kopien, soweit dies (i) technisch durchführbar und vernünftigerweise wirtschaftlich zumutbar ist und (ii) keine Verpflichtung zur Speicherung der personenbezogenen Daten nach dem Unionsrecht oder dem anwendbaren Recht der Mitgliedstaaten besteht.

6. Wir stellen Ihnen Informationen auf Ihr Verlangen zur Verfügung, soweit diese zum Nachweis der Einhaltung Ihrer in Artikel 28 DSGVO niedergelegten Pflichten erforderlich sind.

7. Wir ermöglichen Überprüfungen durch Sie oder einen von Ihnen beauftragten Prüfer, soweit diese ausschließlich dem Zweck des Nachweises der Einhaltung der Pflichten des Artikel 28 DSGVO dienen. Sie führen Überprüfungen nur im erforderlichen Umfang durch und nehmen angemessene Rücksicht auf unsere

Betriebsabläufe. Über den Zeitpunkt sowie die Art der Prüfung verständigen wir uns rechtzeitig.

8. Wir informieren Sie unverzüglich, falls wir der Auffassung sind, dass eine Weisung gegen die DSGVO oder gegen andere anwendbare Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

9. Sie genehmigen, dass wir im Rahmen der Auftragsverarbeitung die in **Anlage 2** bezeichneten Unterauftragnehmer einsetzen. Wir ziehen neue Unterauftragnehmer hinzu und/oder ersetzen diese gegebenenfalls, sofern Sie nicht innerhalb von 14 Kalendertagen auf unsere Mitteilung über die Hinzuziehung und/oder Ersetzung eines Unterauftragnehmers hin in Textform widersprechen. Im Falle eines Widerspruchs sind wir berechtigt, den oder die betroffenen Service(s) aus wichtigem Grund zu kündigen. Wir setzen Unterauftragnehmer zur Verarbeitung personenbezogener Daten im Rahmen dieser Auftragsverarbeitung nur ein, soweit wir den Unterauftragnehmern dem Wesen nach mindestens dieselben Datenschutzpflichten auferlegen, die uns nach den Bestimmungen dieser Auftragsverarbeitung treffen.

Anlage 2
Unterauftragnehmer

1. nicos cyber defense GmbH

2. RSA Security Germany GmbH

3. G DATA Advanced Analytics GmbH

4. QuoSec GmbH

Anlage 3
Technische und organisatorische Maßnahmen der nicos AG

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle

Ziel der Zutrittskontrolle ist es, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Maßnahmen:

- Die Rechenzentren, in denen die vereinbarten Services betrieben werden, sind alarmgesichert. Der Zutritt ist nur berechtigten Personen möglich, zusätzlich zum Schlüssel wird ein Code und Token benötigt. Der Kreis dieser Personen ist auf den erforderlichen Personenkreis beschränkt.
- Die Ausgabe der Schlüssel ist geregelt und wird dokumentiert.
- Besucher erhalten einen Besucherausweis und werden durch Mitarbeiter begleitet.
- Zutritt zum Gebäude ist nur mit Schlüssel möglich. Der nicht besetzte Bereich der Büroräume ist außerhalb der Bürozeiten alarmgesichert. Es findet eine Prüfung durch Wachpersonal statt, ob Türen und Fenster nachts verschlossen sind.
- Ein Zutrittskonzept ist vorhanden.

Zugangskontrolle

Ziel der Zugangskontrolle ist es, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Maßnahmen:

- Zugriff auf interne Systeme erfordert eine personalisierte Anmeldung.
- Passwörter müssen definierte Kriterien erfüllen.
- Verschlüsselung von mobilen Endgeräten ist in der IT-Richtlinie geregelt. Laptops und stationäre PC werden vor Ausgabe an die Mitarbeiter verschlüsselt. Sichere Vernichtung von Datenträgern erfolgt über einen zertifizierten Dienstleister (siehe Ziff. 2 Weitergabekontrolle).
- Einsatz von Anti-Viren-Software und Monitoring durch ein SIEM-System.

- Möglichkeit, den Zugang auf bestimmten Bereichen auf definierte Netzwerke zu beschränken.
- Sicherheitsrelevante Aktionen werden protokolliert.
- Authentifikation mit biometrischen Verfahren ist möglich.
- Einsatz von Hardware-Firewalls.

Zugriffskontrolle

Ziel der Zugriffskontrolle ist es, zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Maßnahmen:

- Eingesetzte Anwendungen und Systeme bieten differenzierte Berechtigungs- und Rollensysteme. Die Definition der Rechte erfolgt nach Möglichkeit rollenbasiert. Die Zuweisung der Rechte zu den einzelnen Benutzern erfolgt über die Rollen, bei Bedarf werden zusätzliche Rechte einzelnen Benutzern zugewiesen.
- Die Vergabe der Berechtigungen erfolgt an zentraler Stelle und ist über ein Zugriffskonzept und einen Berechtigungsprozess geregelt.
- Anzahl der Administratoren ist auf das „notwendigste“ reduziert.
- Einsatz von verschlüsselten mobilen Datenträgern z.B. verschlüsselte USB-Sticks.
- Verwaltung der Rechte durch ausgewählte Systemadministratoren.
- Vernichtung von Akten und Datenträgern über verschlossene Datenschutztonnen (siehe Ziff. 2 Weitergabekontrolle). Der Zugriff auf die Daten ist zeitlich beschränkt und die Daten werden nach Ablauf einer definierten Zeitspanne gemäß des Löschkonzeptes gelöscht. Die Verarbeitung der Daten erfolgt überwiegend maschinell. Eine manuelle Verarbeitung ist im Alarmfall oder beim sogenannten Threat Hunting erforderlich.

Trennungskontrolle

Ziel der Trennungskontrolle ist es, zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Maßnahmen:

- Daten werden durch Zugriffsregelungen getrennt gespeichert.

- Festlegung von Datenbankrechten.
- Produktiv-, Test- und Entwicklungssysteme werden getrennt.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle:

Ziel der Weitergabekontrolle ist es, zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Maßnahmen:

- Fernzugriff auf die DV-Systeme ist nur über gesicherte bzw. verschlüsselte Verbindungen möglich.
- Verschlüsselung von mobilen Endgeräten ist in der IT-Richtlinie geregelt. Laptops und stationäre PC werden vor Ausgabe an die Mitarbeiter verschlüsselt.
- Verschlüsselung und elektronische Signatur von E-Mails ist mittels Zertifikat möglich und wird in der IT-Richtlinie sowie Datenschutzrichtlinie geregelt. Ausgenommen davon ist das Ticketsystem. Ist eine Verschlüsselung mittels Zertifikat nicht möglich, werden die Daten in einer verschlüsselten, mit Passwort geschützten Datei versendet.
- Vernichtung von Informationen in Papierform über verschlossene Datenschutztonnen. Entsorgung erfolgt durch einen Dienstleister. Unser Dienstleister ist nach ISO 9001 zertifiziert und wird regelmäßig auditiert. Die Mitarbeiter sind zur Einhaltung des Datenschutzrechts verpflichtet. Die Vernichtung der Datenträger erfolgt nach DIN66399-2 Sicherheitsstufe P-4. Damit stellt die Firma sicher, dass unsere Daten sicher entsorgt werden.

Eingabekontrolle

Ziel der Eingabekontrolle ist es, zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Maßnahmen:

- Vergabe von Rechten zur Eingabe, Änderung und Löschung (Lese-/Schreibrechte) von Daten auf Basis des Berechtigungskonzepts.

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle

Ziel der Verfügbarkeitskontrolle ist es, zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Maßnahmen:

- Verfügbarkeit der Systeme durch redundante Systeme und Backups. Einsatz einer unterbrechungsfreien Stromversorgung (USV)
- Klimatisierte Serverräume mit Feuermeldeanlagen.
- Feuerlöschgeräte in den Serverräumen vorhanden.
- In den Serverräumen werden Schutzsteckdosen eingesetzt.
- Alarmierung bei unberechtigten Zutritten zu Serverräumen.
- Aufbewahrung der Datensicherungen getrennt in einem Safe.
- Updates der Software werden regelmäßig, zeitnah und zentral eingespielt.

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

Maßnahmen:

- Verfügbarkeit der Systeme durch redundante Systeme und regelmäßige Backups.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Datenschutz-Management

Maßnahmen:

- Es existiert ein Datenschutzmanagementsystem, welches regelmäßig überprüft und aktualisiert wird.

Auftragskontrolle

Ziel der Auftragskontrolle ist es, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Maßnahmen:

- Alle Mitarbeiter werden zu Beginn ihrer Tätigkeit auf das Datengeheimnis verpflichtet.
- Datenschutzbeauftragter ist schriftlich bestellt.