

Auftragsverarbeitungsvertrag (AVV) / Data Processing Agreement (DPA)

NOTE: English translation is available for informational purposes only and is written after the legally binding German version. (see § 11 (5) of this agreement)

zwischen

NeoProtect GmbH,
Ulrichsberger Straße 17,
94469 Deggendorf,
Deutschland,
registriert am AG Deggendorf unter HRB Nummer 6544,
vertreten durch die Geschäftsführer Kilian Pronold und Noah Kolossa
– nachfolgend „**Auftragsverarbeiter**“ –

und

dem Kunden gemäß den geltenden Allgemeinen Geschäftsbedingungen (AGB) des
Auftragsverarbeiters und/oder dem jeweiligen Angebot
– nachfolgend „**Verantwortlicher**“ –

– gemeinsam „**Parteien**“ –

Hinweis: Dieser Vertrag gilt ausschließlich für Kunden, die als Unternehmen, juristische Personen oder sonstige nicht-private Auftraggeber handeln (B2B). Privatpersonen, die NeoProtect-Dienste ausschließlich für private Zwecke nutzen, sind keine Verantwortlichen im Sinne dieses Vertrags; ihre datenschutzrechtlichen Rechte und Pflichten richten sich ausschließlich nach der Datenschutzerklärung unter <https://neoprotect.net/privacy>.

§1 Gegenstand und Dauer

(1) Dieser Vertrag regelt die datenschutzrechtlichen Pflichten der Parteien im Zusammenhang mit der Erbringung der vereinbarten Dienste durch den Auftragsverarbeiter, insbesondere der Bereitstellung des technischen Kundensupports.

(2) Die Laufzeit dieses Vertrags entspricht der Laufzeit der zwischen den Parteien vereinbarten Serviceleistung gemäß den geltenden AGB und/oder dem jeweiligen Angebot.

§2 Art, Zweck und Umfang der Verarbeitung

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Rahmen der Erbringung der vertraglich vereinbarten Dienste für den Verantwortlichen. Die Verarbeitung umfasst insbesondere:

- **Kategorien personenbezogener Daten:** IP-Adressen sowie sonstige Netzwerkdaten (z. B. Packet Dumps, Traffic-Metadaten, Routing-Informationen), soweit sie sich auf identifizierte oder identifizierbare natürliche Personen beziehen; sonstige vom Verantwortlichen im Rahmen der Nutzung der Dienste oder von Support-Tickets übermittelte Daten, die personenbezogene Informationen enthalten können.
- **Kategorien betroffener Personen:** Endnutzer, Netzwerkteilnehmer und sonstige natürliche Personen, deren personenbezogene Daten im Rahmen der Dienstleistung oder der Bearbeitung von Support-Anfragen verarbeitet werden.
- **Zweck der Verarbeitung:** Erbringung des vertraglich vereinbarten Schutz- und Infrastrukturdienstes (insbesondere DDoS-Mitigation, Traffic-Routing, Filterung), Analyse, Diagnose und Behebung technischer Störungen sowie Erbringung der vertraglich geschuldeten Support-Leistungen.

(2) Der Umfang der Verarbeitung im Rahmen des Kerndienstes beschränkt sich auf die technisch notwendige Weiterleitung, Analyse und kurzfristige Zwischenspeicherung personenbezogener Daten zur Erbringung des Schutzdienstes.

(3) Der Verantwortliche ist allein dafür verantwortlich, dass die im Rahmen der Nutzung der Dienste und im Rahmen von Support-Anfragen übermittelten personenbezogenen Daten rechtmäßig erhoben wurden und deren Verarbeitung durch den Auftragsverarbeiter auf einer gültigen Rechtsgrundlage beruht. Der Auftragsverarbeiter ist nicht verpflichtet, die Zulässigkeit der übermittelten Daten inhaltlich zu prüfen.

(4) Die Übermittlung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO ist nicht Gegenstand dieses Vertrags und soll unterbleiben, sofern die Parteien keine gesonderte, ausdrücklich als solche bezeichnete Vereinbarung mit ergänzenden technischen und organisatorischen Maßnahmen treffen. Übermittelt der Verantwortliche gleichwohl solche Daten ohne eine entsprechende Vereinbarung, trägt er hierfür die alleinige Verantwortung. Der Auftragsverarbeiter ist berechtigt, die Verarbeitung dieser Daten abzulehnen und deren unverzügliche Löschung zu verlangen, soweit dem keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

§3 Weisungsgebundenheit

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen. Die zwischen den Parteien geltenden AGB sowie dieser Vertrag gelten als initiale und abschließende Weisung für den Regelbetrieb; darüber hinausgehende Weisungen sind vom Verantwortlichen schriftlich oder in Textform zu erteilen.

(2) Erscheint dem Auftragsverarbeiter eine Weisung offensichtlich rechtswidrig, so weist er den Verantwortlichen hierauf hin; eine eigene rechtliche Prüfungspflicht des

Auftragsverarbeiters besteht nicht. Bis zur Bestätigung oder Änderung der Weisung durch den Verantwortlichen ist der Auftragsverarbeiter berechtigt, die Ausführung der betroffenen Weisung auszusetzen. Erscheint die Ausführung dem Auftragsverarbeiter rechtlich unzulässig, ist er berechtigt, die Ausführung der betroffenen Weisung abzulehnen; hält der Verantwortliche die Weisung nach dem Hinweis ausdrücklich aufrecht, trägt er die datenschutzrechtliche Verantwortung für deren Ausführung. Eine gesetzliche Verpflichtung des Auftragsverarbeiters zur Verarbeitung ohne Weisung besteht nur, soweit das Recht der Union oder der Mitgliedstaaten dies vorschreibt; in diesem 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.

(3) Der Verantwortliche benennt dem Auftragsverarbeiter auf dessen Verlangen eine oder mehrere weisungsberechtigte Personen. Personelle Änderungen teilt der Verantwortliche dem Auftragsverarbeiter unverzüglich in Textform mit. Der Auftragsverarbeiter darf darauf vertrauen, dass über die im Kundenkonto hinterlegten oder gemäß §13 mitgeteilten Kontaktwege erteilte Weisungen von einer berechtigten Person stammen.

(4) Weisungen sind grundsätzlich schriftlich oder in Textform (E-Mail genügt) zu erteilen. Mündliche Weisungen sind nur in begründeten Eilfällen zulässig und vom Verantwortlichen unverzüglich in Textform zu bestätigen. Bis zum Eingang der Bestätigung ist der Auftragsverarbeiter berechtigt, die Ausführung auszusetzen. Der Auftragsverarbeiter protokolliert Person, Datum und Inhalt einer mündlichen Weisung in angemessener Form.

§4 Vertraulichkeit

Der Auftragsverarbeiter stellt sicher, dass alle Personen, die zur Verarbeitung der übermittelten personenbezogenen Daten befugt sind, einer angemessenen Vertraulichkeitsverpflichtung unterliegen.

§5 Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO. Die aktuell geltenden Maßnahmen sind in der Datenschutzerklärung unter <https://neoprotect.net/privacy> beschrieben und können auf Anfrage gesondert zur Verfügung gestellt werden. Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage eine datierte Zusammenfassung der jeweils geltenden technischen und organisatorischen Maßnahmen zur Verfügung. Die zum Zeitpunkt des Vertragsschlusses gültige Fassung wird im Kundenportal als versioniertes Dokument bereitgestellt oder dem Verantwortlichen bei Vertragsschluss übermittelt. Wesentliche Änderungen der Maßnahmen werden dokumentiert; der Verantwortliche erhält auf Anfrage eine Übersicht der Änderungen.

(2) Der Auftragsverarbeiter ist berechtigt, die Maßnahmen weiterzuentwickeln, sofern das Schutzniveau nicht unterschritten wird.

§6 Unterauftragsverarbeiter

(1) Der Auftragsverarbeiter ist berechtigt, Unterauftragsverarbeiter einzusetzen. Die aktuell eingesetzten Unterauftragsverarbeiter sind in der Datenschutzerklärung unter <https://neoprotect.net/privacy> aufgeführt.

(2) Über beabsichtigte Änderungen informiert der Auftragsverarbeiter durch Aktualisierung der Datenschutzerklärung oder per E-Mail.

(3) Der Verantwortliche kann Änderungen innerhalb von 30 Tagen nach Bekanntgabe schriftlich widersprechen. Widerspricht der Verantwortliche fristgerecht und lässt sich der betroffene Unterauftragsverarbeiter nicht durch einen gleichwertigen ersetzen, ist der Auftragsverarbeiter berechtigt, den betroffenen Dienst mit einer Frist von 30 Tagen zu kündigen. Alle Unterauftragsverarbeiter werden zu gleichwertigen datenschutzrechtlichen Pflichten verpflichtet.

(4) Eine Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation findet nur statt, soweit die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (insbesondere Angemessenheitsbeschluss oder Standardvertragsklauseln der EU-Kommission). Die eingesetzten Unterauftragsverarbeiter, ihr jeweiliger Verarbeitungsstandort sowie der für etwaige Drittlandübermittlungen maßgebliche Transfermechanismus sind in der Datenschutzerklärung unter <https://neoprotect.net/privacy> im Abschnitt zu den Unterauftragsverarbeitern und Drittlandübermittlungen tabellarisch aufgeführt.

§7 Unterstützung des Verantwortlichen

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen des technisch und organisatorisch Möglichen bei der Erfüllung von Betroffenenrechten (Art. 15–22 DSGVO) sowie bei den Pflichten gemäß Art. 32–36 DSGVO.

(2) Für Unterstützungsleistungen, die über den gewöhnlichen Leistungsumfang hinausgehen, kann der Auftragsverarbeiter einen angemessenen Aufwandsersatz in Rechnung stellen.

§8 Meldung von Datenschutzverletzungen

Der Auftragsverarbeiter meldet dem Verantwortlichen Verletzungen des Schutzes personenbezogener Daten unverzüglich nach Kenntnis durch die intern zuständige Stelle, in der Regel innerhalb von 72 Stunden. Sollte eine vollständige Meldung innerhalb dieser Frist nicht möglich sein, erfolgt zunächst eine vorläufige Meldung mit den zu diesem Zeitpunkt verfügbaren Informationen; die vollständige Meldung wird unverzüglich nachgereicht, sobald weitere Informationen vorliegen.

§9 Löschung und Datenexport

(1) Löschung und Export personenbezogener Daten erfolgen ausschließlich nach den Verfahren und Fristen, wie sie in der jeweils aktuellen Datenschutzerklärung des Auftragsverarbeiters unter <https://neoprotect.net/privacy> beschrieben sind. Nach Wahl des

Verantwortlichen löscht der Auftragsverarbeiter die personenbezogenen Daten oder gibt sie zurück und löscht vorhandene Kopien, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht.

(2) Maßgeblich sind insbesondere die dort geregelten Speicherdauern, Löschantragsverfahren sowie die Self-Service-Exportfunktion.

(3) Mit Beendigung der Servicelaufzeit gelten die dort beschriebenen Verfahren entsprechend.

(4) Der Auftragsverarbeiter bestätigt dem Verantwortlichen die vollständige Löschung oder Rückgabe der personenbezogenen Daten nach Beendigung der Servicelaufzeit unaufgefordert in Textform. Die Bestätigung benennt den Zeitpunkt und den Umfang der Löschung sowie etwaige aufgrund gesetzlicher Aufbewahrungspflichten zurückbehaltene Daten. Auf Anfrage stellt der Auftragsverarbeiter dem Verantwortlichen die zur Erfüllung von dessen Nachweis- und Kontrollpflichten erforderlichen ergänzenden Informationen zur Verfügung.

§10 Nachweispflichten und Prüfungen

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen auf schriftliche Anfrage die erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO unentgeltlich zur Verfügung. Als Nachweis dienen insbesondere die Zusammenfassung der technischen und organisatorischen Maßnahmen gemäß §5 Abs. 1, die Angaben zu Unterauftragsverarbeitern und Drittlandübermittlungen gemäß §6 sowie vorhandene Zertifizierungen, Testate und Prüfberichte unabhängiger Dritter (Art. 28 Abs. 5 DSGVO). Weitergehende Audits sind zulässig, soweit der Verantwortliche durch diese Nachweise nicht in die Lage versetzt wird, die Einhaltung dieses Vertrags zu beurteilen; sie erfolgen nach schriftlicher Ankündigung mit mindestens 30 Tagen Vorlauf und während der üblichen Geschäftszeiten und vorrangig als Fernprüfung, soweit diese zur Beurteilung ausreicht. Der Verantwortliche ist berechtigt, höchstens ein Audit pro Kalenderjahr durchzuführen, es sei denn, ein konkreter Anlass – insbesondere eine dem Auftragsverarbeiter zuzurechnende Datenschutzverletzung oder eine behördliche Anfrage – erfordert eine zusätzliche Prüfung. Die Dauer eines einzelnen Audits ist auf maximal zwei aufeinanderfolgende Arbeitstage begrenzt, sofern nicht im Einzelfall etwas anderes vereinbart wird.

(2) Weitergehende Audits sind durch den Verantwortlichen selbst oder durch einen unabhängigen, fachlich qualifizierten Prüfer durchzuführen, der nicht mit dem Auftragsverarbeiter im Wettbewerb steht und der zuvor eine Vertraulichkeitsvereinbarung mit dem Auftragsverarbeiter abgeschlossen hat. Der Auftragsverarbeiter kann einem benannten Prüfer aus sachlichem Grund widersprechen; der Verantwortliche benennt in diesem Fall einen anderen Prüfer.

(3) Die Prüfung und die Feststellungen des Prüfers beschränken sich auf die Verarbeitung für den Verantwortlichen. Nicht Gegenstand der Prüfung sind personenbezogene Daten und Vertragsdaten anderer Kunden des Auftragsverarbeiters, Geschäfts- und Betriebsgeheimnisse – insbesondere Filter- und Mitigationslogik, Angriffssignaturen, Schwellenwerte, Quellcode sowie Detailangaben zu Netztopologie und Kapazitäten – sowie

Zugänge, deren Offenlegung die Sicherheit oder Wirksamkeit der Schutzdienste beeinträchtigen könnte; der Auftragsverarbeiter ist berechtigt, Unterlagen insoweit zu schwärzen. Die Prüfung darf den Betrieb des Auftragsverarbeiters nicht unangemessen beeinträchtigen; steht ein laufender Angriff, ein Sicherheitsvorfall oder eine erhebliche Störung entgegen, kann der Auftragsverarbeiter den Termin verschieben und benennt unverzüglich einen Ersatztermin.

(4) Der Auftragsverarbeiter ist berechtigt, den entstehenden Aufwand für weitergehende Audits nach Absatz (1) – einschließlich der Beantwortung von Fragebögen, die über die Nachweise nach Absatz (1) hinausgehen, sowie der Begleitung von Prüfern – zum Stundensatz von 175,00 EUR netto in Rechnung zu stellen. Der geschätzte Aufwand wird dem Verantwortlichen vor Beginn mitgeteilt. Die Kosten des vom Verantwortlichen beauftragten Prüfers trägt der Verantwortliche. Ein Entgelt entfällt, soweit das Audit durch eine dem Auftragsverarbeiter zuzurechnende Datenschutzverletzung oder eine schuldhaft Pflichtenverletzung des Auftragsverarbeiters veranlasst ist.

(5) Der Auftragsverarbeiter ist berechtigt, die anfallenden Kosten vor Beginn eines weitergehenden Audits nach Absatz (1) als Vorauszahlung einzufordern; mit der Auditbegleitung wird erst nach Zahlungseingang begonnen. Dies gilt nicht in den Fällen des Absatzes (4) Satz 4.

(6) Beide Parteien erhalten das Prüfergebnis in identischer Fassung und können hierzu Stellung nehmen. Das Prüfergebnis ist vertraulich zu behandeln; die Verwendung gegenüber Aufsichtsbehörden, Datenschutzbeauftragten, Abschlussprüfern und Rechtsberatern des Verantwortlichen sowie zur Erfüllung eigener gesetzlicher Nachweispflichten bleibt zulässig. Festgestellte Mängel behebt der Auftragsverarbeiter innerhalb angemessener Frist. Prüfungsbefugnisse zuständiger Aufsichtsbehörden (Art. 58 DSGVO) bleiben von diesem §10 unberührt.

§11 Schlussbestimmungen

(1) Dieser Vertrag unterliegt dem Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts (CISG).

(2) Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag ist Deggendorf, Deutschland, sofern der Verantwortliche Kaufmann, juristische Person des öffentlichen Rechts, ein öffentlich-rechtliches Sondervermögen oder Unternehmer im Sinne von § 14 BGB ist.

(3) Sollten einzelne Bestimmungen dieses Vertrags unwirksam oder undurchführbar sein, bleibt der Vertrag im Übrigen wirksam; die unwirksame Bestimmung ist durch eine wirksame zu ersetzen, die dem wirtschaftlichen Zweck am nächsten kommt.

(4) Im Übrigen gelten ergänzend die zwischen den Parteien vereinbarten AGB, soweit sie diesem Vertrag nicht widersprechen. Fragen der Haftung richten sich nach den vereinbarten AGB des Auftragsverarbeiters. Soweit dieser Vertrag datenschutzrechtliche Regelungen enthält, gehen diese im Verhältnis zu den AGB von NeoProtect vor.

(5) Dieser Auftragsverarbeitungsvertrag (AVV) wird in deutscher Sprache verfasst. Die deutschsprachige Fassung ist die allein verbindliche Version. Übersetzungen dienen ausschließlich Informationszwecken.

§12 Änderungen dieses Vertrags

(1) Der Auftragsverarbeiter ist berechtigt, diesen Vertrag anzupassen, sofern dies aufgrund von Änderungen der gesetzlichen oder regulatorischen Anforderungen, des eingesetzten Dienstleistungsumfangs oder der genutzten Unterauftragsverarbeiter erforderlich oder sinnvoll ist.

(2) Über wesentliche Änderungen informiert der Auftragsverarbeiter den Verantwortlichen mindestens 30 Tage vor Inkrafttreten per E-Mail an die im Kundenkonto hinterlegte Adresse. Die jeweils aktuelle Fassung dieses Vertrages ist unter <https://neoprotect.net/dpa> abrufbar.

(3) Widerspricht der Verantwortliche einer Änderung nicht innerhalb von 30 Tagen nach Bekanntgabe in Textform, gilt die geänderte Fassung als angenommen. Auf die Bedeutung des Schweigens wird in der Änderungsmitteilung ausdrücklich hingewiesen.

(4) Im Falle eines fristgerechten Widerspruchs werden die Parteien eine einvernehmliche Lösung suchen; kann keine Einigung erzielt werden, ist jede Partei berechtigt, diesen Auftragsverarbeitungsvertrag (AVV) mit einer Frist von 30 Tagen zu kündigen.

§13 Kommunikation und Formerfordernisse

Sämtliche Mitteilungen, Anzeigen, Anspruchsstellungen, Weisungen sowie sonstige rechtserhebliche Erklärungen im Rahmen dieses Vertrags – einschließlich der Meldung von Datenschutzverletzungen gemäß §8, der Erteilung von Weisungen gemäß §3, der Geltendmachung von Betroffenenrechten gemäß §7 sowie Widersprüche gemäß §6 und §12 – bedürfen der Textform (E-Mail genügt) und sind **kumulativ** an folgende Adressen zu richten:

- dataprotection@neoprotect.net
- legal@neoprotect.net
- Kilian Pronold: kilian@neoprotect.net
- Noah Kolossa: noah@neoprotect.net

Sofern möglich, soll eine solche Mitteilung an alle obigen E-Mail Adressen gesendet werden, mindestens aber an dataprotection@neoprotect.net. Dieser Mindestanforderung muss Folge geleistet werden, um die Bearbeitung sicherzustellen.

Jede Mitteilung muss folgende Mindestanforderungen erfüllen:

1. Eindeutige Betreffzeile mit Bezug auf diesen Vertrag sowie der Kundennummer oder dem im Kundenkonto hinterlegten Unternehmensnamen
2. Klare Bezeichnung des Anliegens – insbesondere ob es sich um eine Weisung, eine Mängelanzeige, eine Anspruchsstellung, einen Widerspruch oder eine Datenschutzmeldung handelt

3. Vollständige Sachverhaltsdarstellung mit allen relevanten Informationen, die für die Bearbeitung erforderlich sind, einschließlich Datum, betroffener Systeme oder Personen sowie einer konkreten Beschreibung des Vorfalls oder Begehrens
4. Eindeutige Benennung der gewünschten Maßnahme oder Reaktion sowie einer angemessenen Frist, sofern eine solche gefordert wird
5. Die Kommunikation soll ausschließlich in der Sprache Deutsch oder Englisch vollzogen werden

Bei unvollständigen oder unstrukturierten Mitteilungen kann die empfangende Partei die fehlenden Angaben anfordern; die betroffene Partei ergänzt diese unverzüglich. Der Zeitpunkt des ursprünglichen Zugangs bleibt hiervon unberührt, und gesetzliche Fristen werden durch einen bloßen Formmangel weder gehemmt noch verschoben. Meldungen von Datenschutzverletzungen des Auftragsverarbeiters gemäß §8 sind an den Verantwortlichen über die im Kundenkonto hinterlegten bzw. die vom Verantwortlichen für Datenschutzangelegenheiten benannten Kontaktdaten zu richten; der Verantwortliche hält diese Kontaktdaten aktuell. Dringende sowie datenschutzrechtlich fristgebundene Mitteilungen (insbesondere Meldungen von Datenschutzverletzungen und die Geltendmachung von Betroffenenrechten) sind auch dann wirksam und fristwährend, wenn sie die vorstehenden Formanforderungen nicht vollständig erfüllen.

§14 Vertragsschluss und Wirksamkeit

(1) NeoProtect kann dem Kunden als B2B-Kunde über das Panel (wie in den AGB definiert) die Möglichkeit bereitstellen, diesen Auftragsverarbeitungsvertrag (AVV) abzuschließen.

(2) Der Vertragsschluss erfolgt dadurch, dass der Kunde über das Panel die zur Kenntnisnahme bereitgestellte Fassung dieses Vertrags durch Setzen des dafür vorgesehenen Bestätigungskästchens (Checkbox) sowie durch Anklicken der entsprechenden Bestätigungsschaltfläche (Button) ausdrücklich annimmt.

(3) Dieser Auftragsverarbeitungsvertrag (AVV) wird erst mit der Annahme gemäß Absatz (2) wirksam. Solange kein wirksamer AVV vorliegt, nimmt NeoProtect keine Verarbeitung personenbezogener Daten im Auftrag des B2B-Kunden vor, die einen wirksamen AVV im Sinne von Art. 28 DSGVO voraussetzt. Der gemäß Absatz (4) dokumentierte Annahmenachweis weist den Verantwortlichen, den erfassten Leistungs- und Verarbeitungsumfang, das Datum sowie den angenommenen Versionsstand dieses Vertrags aus.

(4) NeoProtect ist berechtigt, den Zeitpunkt der Annahme sowie den zum Annahmezeitpunkt geltenden Versionsstand dieses Vertrags zu Nachweiszwecken zu dokumentieren und zu speichern.

§15 Anonymisierte und aggregierte Daten

(1) Der Verantwortliche weist den Auftragsverarbeiter hiermit ausdrücklich und als vorformulierte, dokumentierte Weisung im Sinne von §3 an, die im Rahmen der Dienstleistungsbereitstellung Netzwerk- und Traffic-Daten (insbesondere Angriffsmuster, Traffic-Metadaten, Anomalie- und Bedrohungsindikatoren) zu anonymisieren, d. h. so zu

verändern, dass ein Personenbezug unwiderruflich und auch unter Berücksichtigung des nach allgemeinem Ermessen wahrscheinlich einzusetzenden Zusatzwissens nicht mehr hergestellt werden kann. Eine bloße Pseudonymisierung genügt hierfür nicht.

(2) Die Anonymisierung nach Absatz (1) erfolgt zum Zweck der Gewährleistung und Verbesserung der IT- und Netzwerksicherheit, der Erkennung und Abwehr von Angriffen (Threat Intelligence), der Weiterentwicklung und Optimierung der Schutzdienste sowie zu statistischen Zwecken.

(3) Der Vorgang der Anonymisierung nach Absatz (1) ist selbst eine Verarbeitung personenbezogener Daten. Soweit der Auftragsverarbeiter diesen Vorgang zu den in Absatz (2) genannten eigenen Zwecken (insbesondere Threat Intelligence und Verbesserung der Schutzdienste) durchführt, handelt er hinsichtlich dieses Anonymisierungsvorgangs als eigenständig Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO. Rechtsgrundlage dieser Verarbeitung ist Art. 6 Abs. 1 lit. f DSGVO; das berechtigte Interesse des Auftragsverarbeiters liegt in der Gewährleistung und Verbesserung der IT- und Netzwerksicherheit sowie der Abwehr von Angriffen. Der Auftragsverarbeiter beschränkt diese Verarbeitung auf das hierfür erforderliche Maß, trifft geeignete technische und organisatorische Schutzmaßnahmen und informiert betroffene Personen im Rahmen seiner eigenen Datenschutzhinweise transparent hierüber. Die aus der Anonymisierung hervorgehenden Daten weisen keinen Personenbezug mehr auf und unterfallen nicht mehr dem Anwendungsbereich der DSGVO; der Auftragsverarbeiter ist berechtigt, diese anonymisierten und/oder aggregierten Daten zeitlich unbegrenzt und ohne Nennung des Verantwortlichen zu nutzen, auszuwerten, mit Daten anderer Quellen zusammenzuführen und in anonymisierter Form an Dritte weiterzugeben oder zu veröffentlichen.

(4) Die eigenständige Verantwortlichkeit des Auftragsverarbeiters nach Absatz (3) betrifft ausschließlich den Anonymisierungsvorgang und die anschließende Nutzung der anonymen Ergebnisse; die vorgelagerte Verarbeitung im Auftrag des Verantwortlichen bleibt hiervon unberührt. Eine gemeinsame Verantwortlichkeit (Art. 26 DSGVO) wird hierdurch nicht begründet; die Parteien legen Zwecke und Mittel dieser Verarbeitung nicht gemeinsam fest.

§16 Haftung und Freistellung

(1) Die Haftung der Parteien richtet sich nach den zwischen ihnen vereinbarten AGB des Auftragsverarbeiters, soweit dieser Vertrag keine abweichenden Regelungen enthält. §11 Abs. 4 bleibt unberührt.

(2) Der Verantwortliche stellt den Auftragsverarbeiter von sämtlichen Ansprüchen Dritter, betroffener Personen oder Aufsichtsbehörden sowie von Bußgeldern frei, die darauf beruhen, dass der Verantwortliche personenbezogene Daten unrechtmäßig erhoben, ohne gültige Rechtsgrundlage übermittelt oder unter Verstoß gegen §2 Abs. 3 und Abs. 4 dieses Vertrags an den Auftragsverarbeiter übergeben hat. Die Freistellung umfasst auch die angemessenen Kosten der Rechtsverteidigung.

(3) Die Freistellung nach Absatz (2) gilt nicht, soweit der Auftragsverarbeiter die Inanspruchnahme durch eine eigene schuldhaftige Pflichtverletzung, insbesondere durch eine



Verletzung seiner Pflichten aus diesem Vertrag oder aus Art. 28, 32 DSGVO, mitverursacht hat; in diesem Fall haftet jede Partei im Umfang ihres jeweiligen Verantwortungsbeitrags.

(4) Im Innenverhältnis der Parteien richtet sich ein Ausgleich nach Art. 82 Abs. 5 DSGVO nach dem jeweiligen Anteil an der Verantwortung für den eingetretenen Schaden.

Auftragsverarbeitungsvertrag (AVV) / Data Processing Agreement (DPA)

NOTE: This English translation is provided for informational purposes only. The legally binding version is the German version above. (see § 11 (5) of this agreement)

between

NeoProtect GmbH,
Ulrichsberger Straße 17,
94469 Deggendorf,
Germany,
registered with the Local Court (Amtsgericht) of Deggendorf under HRB number 6544,
represented by the Managing Directors Kilian Pronold and Noah Kolossa
– hereinafter „**Processor**“ –

and

the customer in accordance with the applicable General Terms and Conditions (GTC) of the Processor and/or the respective offer
– hereinafter „**Controller**“ –

– jointly the „**Parties**“ –

Note: This agreement applies exclusively to customers acting as enterprises, legal entities, or other non-private clients (B2B). Private individuals who use NeoProtect services exclusively for private purposes are not controllers within the meaning of this agreement; their data protection rights and obligations are governed exclusively by the privacy policy at <https://neoprotect.net/privacy>.

§1 Subject Matter and Term

(1) This agreement governs the data protection obligations of the Parties in connection with the provision of the agreed services by the Processor, in particular the provision of technical customer support.

(2) The term of this agreement corresponds to the term of the service agreed between the Parties in accordance with the applicable GTC and/or the respective offer.

§2 Nature, Purpose, and Scope of the Processing

(1) The processor processes personal data in the course of providing the contractually agreed services for the controller. The processing comprises, in particular:

- **Categories of personal data:** IP addresses and other network data (e.g., packet dumps, traffic metadata, routing information) insofar as they relate to identified or identifiable natural persons; other data transmitted by the controller in the course of using the services or via support tickets that may contain personal information.
- **Categories of data subjects:** End users, network participants, and other natural persons whose personal data are processed in the course of service provision or the handling of support requests.
- **Purpose of processing:** Provision of the contractually agreed protection and infrastructure service (specifically DDoS mitigation, traffic routing, filtering), analysis, diagnosis, and resolution of technical issues, as well as provision of the contractually owed support services.

(2) The scope of processing within the core service is limited to the technically necessary forwarding, analysis, and short-term caching of personal data for the purpose of providing the protection service.

(3) The Controller is solely responsible for ensuring that personal data transmitted in connection with the use of the services and support requests have been collected lawfully and that their processing by the Processor is based on a valid legal basis. The Processor is under no obligation to verify the substantive admissibility of the transmitted data.

(4) The transmission of special categories of personal data within the meaning of Art. 9(1) GDPR is not covered by this Agreement and must be avoided unless the parties enter into a separate agreement—expressly designated as such—containing supplementary technical and organizational measures. Should the Controller nevertheless transmit such data without such an agreement, it bears sole responsibility for doing so. The Processor is entitled to refuse the processing of such data and to demand their immediate deletion, provided that no statutory retention obligations prevent this.

§3 Bound by Instructions

(1) The Processor processes personal data exclusively on the documented instructions of the Controller. The GTC applicable between the Parties as well as this agreement are deemed the initial and final instruction for regular operations; any instructions going beyond this are to be issued by the Controller in writing or in text form.

(2) If an instruction appears to the Processor to be manifestly unlawful, it shall notify the Controller thereof; the Processor is under no obligation to carry out its own legal assessment. Until the instruction is confirmed or amended by the Controller, the Processor is entitled to suspend execution of the affected instruction. If execution appears to the Processor to be legally impermissible, it is entitled to refuse to execute the affected instruction; if the Controller expressly upholds the instruction after being notified, the Controller bears data protection responsibility for its execution. The Processor is only obliged to process without instructions where Union or Member State law so requires; in that case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

(3) At the Processor's request, the Controller designates one or more persons authorized to issue instructions. The Controller notifies the Processor of any personnel changes without undue delay in text form. The Processor may rely on the assumption that instructions issued via the contact channels stored in the customer account or communicated pursuant to §13 originate from an authorized person.

(4) Instructions are, as a rule, to be issued in writing or in text form (e-mail is sufficient). Oral instructions are permissible only in justified urgent cases and must be confirmed by the Controller in text form without undue delay. Until receipt of such confirmation, the Processor is entitled to suspend execution. The Processor documents the person, date, and content of an oral instruction in an appropriate form.

§4 Confidentiality

The Processor ensures that all persons authorized to process the transmitted personal data are subject to an appropriate confidentiality obligation.

§5 Technical and Organizational Measures

(1) The Processor takes appropriate technical and organizational measures pursuant to Art. 32 GDPR. The currently applicable measures are described in the privacy policy at <https://neoprotect.net/privacy> and can be made available separately upon request. Upon request, the processor shall provide the controller with a dated summary of the technical and organizational measures currently in force. The version valid at the time of contract conclusion is made available in the customer portal as a versioned document or transmitted to the controller upon conclusion of the contract. Material changes to the measures are documented; the controller receives an overview of the changes upon request.

(2) The Processor is entitled to further develop the measures, provided that the level of protection is not reduced below the agreed standard.

§6 Sub-processors

(1) The Processor is entitled to engage sub-processors. The sub-processors currently engaged are listed in the privacy policy at <https://neoprotect.net/privacy>.

(2) The Processor informs about intended changes by updating the privacy policy or by e-mail.

(3) The Controller may object to changes in writing within 30 days of notification. If the Controller objects in good time and the sub-processor concerned cannot be replaced by an equivalent one, the Processor is entitled to terminate the affected service with a notice period of 30 days. All sub-processors are bound to equivalent data protection obligations.

(4) A transfer of personal data to a third country or an international organization takes place only insofar as the requirements of Art. 44 et seq. GDPR are met (in particular an adequacy decision or the EU Commission's standard contractual clauses). The engaged sub-processors, their respective processing location, and the transfer mechanism relevant

for any third-country transfers are listed in tabular form in the privacy policy at <https://neoprotect.net/privacy> in the section on sub-processors and third-country transfers.

§7 Support of the Controller

(1) The Processor supports the Controller, within the scope of what is technically and organizationally possible, in fulfilling data subject rights (Art. 15–22 GDPR) as well as the obligations pursuant to Art. 32–36 GDPR.

(2) For support services that go beyond the ordinary scope of services, the Processor may invoice an appropriate reimbursement of expenses.

§8 Notification of Data Breaches

The processor shall notify the controller of personal data breaches without undue delay after becoming aware of them through the internally responsible unit—as a rule, within 72 hours. If a complete notification is not possible within this timeframe, an initial preliminary notification shall be provided containing the information available at that time; the complete notification shall follow without undue delay as soon as further information becomes available.

§9 Deletion and Data Export

(1) Deletion and export of personal data are carried out exclusively in accordance with the procedures and periods as described in the Processor's privacy policy as amended from time to time at <https://neoprotect.net/privacy>. At the Controller's choice, the Processor deletes the personal data or returns it and deletes existing copies, provided that no statutory retention obligation conflicts with this.

(2) Decisive are in particular the storage periods, deletion request procedures, and the self-service export function regulated therein.

(3) Upon termination of the service term, the procedures described therein apply accordingly.

(4) The Processor confirms to the Controller, unsolicited and in text form, the complete deletion or return of the personal data upon termination of the service term. The confirmation states the time and scope of the deletion as well as any data retained due to statutory retention obligations. Upon request, the Processor provides the Controller with the supplementary information necessary to fulfill the Controller's evidence and control obligations.

§10 Obligations to Provide Evidence and Audits

(1) Upon written request, the Processor makes available to the Controller the information necessary to demonstrate compliance with the obligations under Art. 28 GDPR free of charge. Such evidence consists in particular of the summary of the technical and organizational measures pursuant to §5(1), the information on sub-processors and third-country transfers pursuant to §6, as well as any existing certifications, attestations, and audit reports of independent third parties (Art. 28(5) GDPR). Further audits are permissible

insofar as this evidence does not enable the Controller to assess compliance with this agreement; they take place after written notice of at least 30 days in advance and during normal business hours and primarily as a remote audit where this is sufficient for the assessment. The controller is entitled to conduct a maximum of one audit per calendar year, unless a specific event—in particular a data protection breach attributable to the processor or an inquiry by a public authority—necessitates an additional audit. The duration of a single audit is limited to a maximum of two consecutive working days, unless otherwise agreed in an individual case.

(2) Further audits shall be conducted by the Controller itself or by an independent, professionally qualified auditor who is not a competitor of the Processor and who has previously entered into a confidentiality agreement with the Processor. The Processor may object to a designated auditor on objective grounds; in this case, the Controller designates another auditor.

(3) The audit and the auditor's findings are limited to the processing carried out for the Controller. Not subject to the audit are personal data and contract data of other customers of the Processor, trade and business secrets – in particular filtering and mitigation logic, attack signatures, thresholds, source code, and detailed information on network topology and capacities – as well as access whose disclosure could impair the security or effectiveness of the protection services; the Processor is entitled to redact documents accordingly. The audit must not unreasonably impair the Processor's operations; if an ongoing attack, a security incident, or a significant disruption prevents proper performance, the Processor may postpone the appointment and shall designate a replacement date without undue delay.

(4) The Processor is entitled to invoice the expenses incurred for further audits pursuant to paragraph (1) – including answering questionnaires that go beyond the evidence under paragraph (1) and accompanying auditors – at an hourly rate of EUR 175.00 net. The estimated expense is communicated to the Controller before commencement. The costs of the auditor engaged by the Controller are borne by the Controller. No fee applies insofar as the audit is occasioned by a personal data breach attributable to the Processor or by a culpable breach of duty by the Processor.

(5) The Processor is entitled to demand the costs incurred as an advance payment before commencing a further audit pursuant to paragraph (1); the audit support begins only after receipt of payment. This does not apply in the cases of paragraph (4), sentence 4.

(6) Both Parties receive the audit result in identical form and may comment on it. The audit result is to be treated as confidential; its use for supervisory authorities, data protection officers, statutory auditors, and legal advisors of the Controller, as well as for the fulfillment of the Controller's own statutory documentation obligations, remains permissible. The Processor remedies identified deficiencies within a reasonable period. The investigative powers of competent supervisory authorities (Art. 58 GDPR) remain unaffected by this §10.

§11 Final Provisions

(1) This agreement is governed by the law of the Federal Republic of Germany, excluding the UN Convention on Contracts for the International Sale of Goods (CISG).

(2) The exclusive place of jurisdiction for all disputes arising from or in connection with this contract is Deggendorf, Germany, provided that the responsible party is a merchant, a legal entity under public law, a special fund under public law, or an entrepreneur within the meaning of § 14 BGB.

(3) Should individual provisions of this agreement be invalid or unenforceable, the agreement otherwise remains effective; the invalid provision is to be replaced by a valid one that most closely approximates the economic purpose.

(4) In all other respects, the GTC agreed between the Parties apply additionally, insofar as they do not contradict this agreement. Questions of liability are governed by the agreed GTC of the Processor. To the extent that this contract contains provisions regarding data protection, these take precedence over NeoProtect's General Terms and Conditions.

(5) This Data Processing Agreement (DPA) is drawn up in the German language. The German-language version is the sole binding version. Translations serve informational purposes only.

§12 Amendments to this Agreement

(1) The Processor is entitled to adapt this agreement, provided that this is necessary or expedient due to changes in legal or regulatory requirements, the scope of services used, or the sub-processors used.

(2) The Processor informs the Controller of material changes at least 30 days before they take effect by e-mail to the address stored in the customer account. The current version of this contract is available at <https://neoprotect.net/dpa>.

(3) If the Controller does not object to a change in text form within 30 days of notification, the amended version is deemed accepted. The significance of silence is expressly pointed out in the change notification.

(4) In the event of a timely objection, the Parties will seek an amicable solution; if no agreement can be reached, either Party is entitled to terminate this Data Processing Agreement (DPA) with a notice period of 30 days.

§13 Communication and Formal Requirements

All notifications, notices, assertions of claims, instructions, and other legally relevant declarations within the scope of this agreement – including the notification of data breaches pursuant to §8, the issuing of instructions pursuant to §3, the assertion of data subject rights pursuant to §7, as well as objections pursuant to §6 and §12 – require text form (e-mail is sufficient) and are to be addressed **cumulatively** to the following addresses:

- dataprotection@neoprotect.net
- legal@neoprotect.net
- Kilian Pronold: kilian@neoprotect.net

- Noah Kolossa: noah@neoprotect.net

Where possible, such a notification should be sent to all of the above e-mail addresses, but at least to dataprotection@neoprotect.net. This minimum requirement must be complied with in order to ensure processing.

Each notification must meet the following minimum requirements:

1. A clear subject line referring to this agreement as well as the customer number or the company name stored in the customer account
2. A clear designation of the matter – in particular whether it concerns an instruction, a notice of defect, an assertion of a claim, an objection, or a data breach notification
3. A complete description of the facts with all relevant information required for processing, including the date, the systems or persons concerned, as well as a concrete description of the incident or request
4. A clear designation of the desired measure or response, as well as an appropriate deadline, if such is required
5. Communication shall be conducted exclusively in German or English

In the case of incomplete or unstructured communications, the receiving Party may request the missing information; the Party concerned shall supplement it without undue delay. The time of the original receipt remains unaffected, and statutory deadlines are neither suspended nor postponed by a mere formal defect. Notifications of personal data breaches by the Processor pursuant to §8 shall be addressed to the Controller via the contact details designated by the Controller. Urgent communications and those subject to statutory data protection deadlines (in particular notifications of personal data breaches and the exercise of data subject rights) are effective and preserve deadlines even if they do not fully meet the foregoing formal requirements.

§14 Conclusion and Effectiveness of the Agreement

(1) NeoProtect may provide the customer, as a B2B customer, with the option to conclude this Data Processing Agreement (DPA) via the Panel (as defined in the GTC).

(2) The agreement is concluded by the customer expressly accepting the version of this agreement made available for review via the Panel, by ticking the designated confirmation checkbox and by clicking the corresponding confirmation button.

(3) This Data Processing Agreement (DPA) becomes effective only upon acceptance in accordance with paragraph (2). As long as no effective DPA is in place, NeoProtect does not carry out any processing of personal data on behalf of the B2B customer that requires an effective DPA within the meaning of Art. 28 GDPR. The acceptance record documented pursuant to paragraph (4) identifies the Controller, the services and processing scope covered, the date, and the accepted version of this Agreement.

(4) NeoProtect is entitled to document and store the time of acceptance as well as the version identifier of this agreement valid at the time of acceptance for evidentiary purposes.

§15 Anonymized and Aggregated Data

(1) The Controller hereby expressly instructs the Processor, as a pre-formulated, documented instruction within the meaning of §3, to anonymize the network and traffic data processed in the course of service provision (in particular attack patterns, traffic metadata, anomaly and threat indicators), i.e. to alter them in such a way that a personal reference can no longer be established irreversibly and even taking into account the additional knowledge likely to be used according to general discretion. Mere pseudonymization is not sufficient for this purpose.

(2) The anonymization pursuant to paragraph (1) is carried out for the purpose of ensuring and improving IT and network security, detecting and mitigating attacks (threat intelligence), further developing and optimizing the protection services, and for statistical purposes.

(3) The act of anonymization pursuant to paragraph (1) is itself a processing of personal data. Insofar as the Processor carries out this act for its own purposes set out in paragraph (2) (in particular threat intelligence and improvement of the protection services), it acts, with respect to this anonymization activity, as an independent controller within the meaning of Art. 4(7) GDPR. The legal basis for this processing is Art. 6(1)(f) GDPR; the Processor's legitimate interest lies in ensuring and improving IT and network security and in mitigating attacks. The Processor limits this processing to what is necessary for that purpose, takes appropriate technical and organizational safeguards, and informs data subjects transparently thereof in its own privacy notice. The data resulting from the anonymization no longer have any personal reference and no longer fall within the scope of the GDPR; the Processor is entitled to use, analyze, combine with data from other sources, and pass on to third parties or publish such anonymized and/or aggregated data in anonymized form, without any time limit and without naming the Controller.

(4) The Processor's independent controllership under paragraph (3) concerns solely the anonymization activity and the subsequent use of the anonymous results; the upstream processing on behalf of the Controller remains unaffected. This does not establish joint controllership (Art. 26 GDPR); the Parties do not jointly determine the purposes and means of this processing.

§16 Liability and Indemnification

(1) The liability of the Parties is governed by the GTC of the Processor agreed between them, insofar as this agreement does not contain any deviating provisions. §11(4) remains unaffected.

(2) The Controller indemnifies the Processor against all claims by third parties, data subjects, or supervisory authorities, as well as against fines, that are based on the Controller having collected personal data unlawfully, transmitted it without a valid legal basis, or handed it over to the Processor in breach of §2(3) and (4) of this agreement. The indemnification also covers the reasonable costs of legal defense.

(3) The indemnification pursuant to paragraph (2) does not apply insofar as the Processor has contributed to the claim through its own culpable breach of duty, in particular through a

breach of its obligations under this agreement or under Art. 28, 32 GDPR; in such a case, each Party is liable to the extent of its respective contribution to the responsibility.

(4) In the internal relationship between the Parties, any settlement pursuant to Art. 82(5) GDPR is based on the respective share of responsibility for the damage incurred.