VERTRAG ZUR AUFTRAGSVERARBEITUNG
NACH ARTIKEL 28 ABSATZ 3 DSGVO

Dieser Vertrag zur Auftragsverarbeitung nach Artikel 28 Absatz 3 DSGVO (nachfolgend „AV-Vertrag“) wird am _____ ("*Datum des Inkrafttretens*") geschlossen

zwischen

_____

- nachfolgend „*Verantwortlicher*“ genannt -

und

VMRay GmbH, HRB 14688, mit Sitz in Universitätsstraße 142, 44799 Bochum, Deutschland

- nachfolgend „*Auftragsverarbeiter*“ genannt -

- sowohl der Verantwortliche als auch der Auftragsverarbeiter werden im Folgenden einzeln als "*Partei*" und gemeinsam als "*Parteien*" bezeichnet -

§ 1 Gegenstand und Dauer der Vereinbarung

(1) Der Auftrag umfasst

☐ die Analyse von Samples / elektronischen Dokumenten des Verantwortlichen, um Cyberbedrohungen zu detektieren und zu analysieren.

☐ folgende Leistungen: _____

(Gegenstand des Auftrags, Beschreibung der Dienstleistungen)

☐ Leistungen gemäß Vertrag _____

(Verweis auf konkreten Hauptvertrag)

(2) Der AV-Vertrag wird auf unbestimmte Zeit geschlossen und endet automatisch mit Beendigung des Hauptvertrages.

§ 2 Kategorien der personenbezogenen Daten, Zweck der Verarbeitung sowie Kategorien betroffener Personen

(1) Die Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DSGVO) beinhaltet folgende Tätigkeiten:

☐ Malwareanalyse (Erkennung und Analyse von Cyberbedrohungen)

☐ _____

(Beschreibung der Art der Verarbeitung)

(2) Die Auftragsverarbeitung umfasst die in der nachstehenden Tabelle aufgeführten Kategorien personenbezogener Daten, den Zweck der Verarbeitung und die Kategorie der betroffenen Personen:

Kategorie der personenbezogenen Daten (Art. 4 Nr. 1, 13, 14 und 15 DSGVO)	Zweck der Verarbeitung	Kategorie der betroffenen Personen (Art. 4 Nr. 1 DSGVO)
Abhängig von der Nutzung des Dienstes durch den Verantwortlichen und den hochgeladenen Daten können die Datenkategorien Namen, E-Mails, Postadressen, URLs und IP-Adressen umfassen, sind aber nicht darauf beschränkt.	*Analyse von Dateien, die möglicherweise mit Malware infiziert sind und personenbezogene Daten enthalten können. Die Übertragung dieser personenbezogenen Daten ist jedoch nur eine unvermeidliche Nebenwirkung dieser Art von Malware-Schutzlösung.*	*Abhängig von der Nutzung des Dienstes durch den Verantwortlichen und den hochgeladenen Daten können zu den betroffenen Personen unter anderem Kunden und Mitarbeiter des Verantwortlichen sowie andere Dritte gehören. Der Auftragsverarbeiter greift jedoch nicht explizit auf diese personenbezogenen Daten zu, verarbeitet oder speichert sie nicht gesondert.*

§ 3 Rechte und Pflichten des Verantwortlichen sowie Zuständigkeitsverteilung

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen. Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Artikel 6 Absatz 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Artikeln 12 bis 22 DSGVO ist allein der Verantwortliche verantwortlich. Der Verantwortliche ist der "für die Verarbeitung Verantwortlicher" im Sinne von Artikel 4 Nr. 7 DSGVO.
(2) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen den Parteien abzustimmen und schriftlich festzulegen.
(3) Der Verantwortliche erteilt alle (Teil-)Aufträge und Weisungen schriftlich oder in einem elektronischen Format. Mündliche Weisungen sind unverzüglich vom Verantwortlichen schriftlich oder in einem elektronischen Format zu bestätigen.
(4) Der Verantwortliche hat den Auftragsverarbeiter unverzüglich über Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse sowie über Verstöße gegen datenschutzrechtliche Bestimmungen zu informieren.
(5) Der Verantwortliche ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragsverarbeiters vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses AV-Vertrages bestehen.
(6) Der Verantwortliche ist berechtigt, sich regelmäßig in angemessener Weise von der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem AV-Vertrag festgelegten Verpflichtungen zu überzeugen (§ 4).

§ 4 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Verantwortlichen, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Europäischen Union oder dem Mitgliedsstaat, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z.B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Artikel 28 Absatz 3 Satz 2 lit. a DSGVO).

(2) Der Auftragsverarbeiter verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Verantwortlichen nicht erstellt.

(3) Der Auftragsverarbeiter verpflichtet sich zur vertragsgemäßen Abwicklung aller vereinbarten Maßnahmen und zur strikten Trennung der verarbeiteten Daten von sonstigen Datenbeständen.

(4) Der Auftragsverarbeiter ist verpflichtet, alle Anfragen, sofern sie erkennbar ausschließlich an den Verantwortlichen gerichtet sind, unverzüglich an diesen weiterzuleiten.

(5) Sofern nicht ausdrücklich durch geltendes Recht erlaubt (z.B. Artikel 28 (3) lit. a der DSGVO), darf der Auftragsverarbeiter personenbezogene Daten über betroffene Personen nur im Rahmen der im Hauptvertrag und der vom Verantwortlichen erteilten Weisungen festgelegten Aufgaben erheben, verarbeiten und nutzen. Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung gegen geltendes Recht verstößt, hat er den Verantwortlichen unverzüglich davon in Kenntnis zu setzen.

(6) Der Auftragsverarbeiter ist verpflichtet, im Rahmen seines Verantwortungsbereichs seine interne Organisation so zu gestalten, dass sie den spezifischen Anforderungen des Schutzes personenbezogener Daten entspricht. Der Auftragsverarbeiter hat technische und organisatorische Maßnahmen zu ergreifen und aufrechtzuerhalten, um die personenbezogenen Daten des Verantwortlichen in Übereinstimmung mit den Anforderungen der DSGVO und insbesondere deren Artikel 32 angemessen zu schützen. Diese Maßnahmen werden wie in der folgenden Liste definiert umgesetzt:

	Maßnahmen
1. Physische Zugangskontrolle:	Elektronische physische Zugangskontrolle (z. B. durch Ausweis- oder Kartenleser) zu den Standorten des Auftragsverarbeiters.
2. Logische Zugriffskontrolle:	Autorisierte Benutzernamen und individuelle Passwörter für den Zugang zu Datenverarbeitungssystemen.
3. Kontrolle des Datenzugriffs:	Hierarchische Zugangskontrollkonzepte mit getrennten Benutzernamen und Passwörtern für den Zugang zu Datenverarbeitungssystemen.
4. Kontrolle der Datenübertragung:	Umsetzung technischer Maßnahmen, die verhindern, dass Unternehmensdaten während der elektronischen Übermittlung oder während des Transports unbefugt verarbeitet oder genutzt werden können (z. B. durch Verschlüsselung oder Passwortschutz).
5. Kontrolle der Dateneingabe:	Prüfung und Aufzeichnung der von den Mitarbeitern des Auftragsverarbeiters durchgeführten Zugriffstransaktionen auf

	die Daten des Unternehmens unter Verwendung von Protokolldateien im Falle der Verarbeitung auf den Systemen des Auftragsverarbeiters.
6. Kontrolle der Verarbeitungsanweisungen:	Unterweisung der Mitarbeiter des Auftragsverarbeiters in Umfang und lnhalt der vom Unternehmen erteilten Anweisungen.
7. Kontrolle der Verfügbarkeit:	Schutz vor Feuer und Maßnahmen bei Stromausfall in den Rechenzentren des Auftragsverarbeiters. Erstellung von Backups (die gemäß dem Handelsvertrag ausgeübt werden).
8. Trennungskontrolle:	Daten verschiedener Kunden werden logisch getrennt gespeichert.

Im Hinblick auf die Schutzmaßnahmen und deren Wirksamkeit hat der Auftragsverarbeiter die Einhaltung der vereinbarten Verpflichtungen mit geeigneten, nach geltendem Recht zulässigen Methoden zu dokumentieren und dem Verantwortlichen auf Anforderung nachzuweisen.

(7) Der Auftragsverarbeiter ist berechtigt, die vereinbarten Maßnahmen zu ändern, wobei jedoch eine Änderung nicht zulässig ist, wenn dadurch das vertraglich vereinbarte Schutzniveau beeinträchtigt wird.

(8) Der Auftragsverarbeiter stellt sicher, dass das mit der Verarbeitung der personenbezogenen Daten des Verantwortlichen betraute Personal (i) sich zur Geheimhaltung verpflichtet hat oder (ii) einer entsprechenden gesetzlichen Geheimhaltungspflicht unterliegt. Die Verpflichtung zur Geheimhaltung besteht auch nach Beendigung der oben genannten Tätigkeiten fort.

(9) Der Auftragsverarbeiter verpflichtet sich zur Einhaltung von Artikel 32 (1) lit. d) DSGVO.

(10) Macht eine betroffene Person Ansprüche gegen den Verantwortlichen nach geltendem Recht geltend, wie z. B. Artikel 82 der DSGVO, so unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Abwehr solcher Ansprüche, soweit dies möglich ist.

§ 5 Verpflichtungen des Auftragsverarbeiters nach Beendigung des Auftrags (Artikel 28 Absatz 3 Satz 2 lit. g DSGVO)

Sofern dies nicht durch geltendes Recht untersagt ist, stellt der Auftragsverarbeiter dem Verantwortlichen nach Beendigung dieses AV-Vertrages auf dessen Anweisung hin alle Daten, Datenträger und andere zugehörige Materialien zur Verfügung oder löscht sie. Sofern im Hauptvertrag nichts anderes vereinbart ist, trägt der Verantwortliche alle zusätzlichen Kosten, die durch die in diesem §5 beschriebene Unterstützung durch den Auftragsverarbeiter verursacht werden.

§ 6 Anfragen von betroffenen Personen

Macht eine betroffene Person gegenüber dem Auftragsverarbeiter Ansprüche auf Berichtigung, Löschung oder Auskunft geltend und ist der Auftragsverarbeiter in der Lage, die betroffene Person anhand der von der betroffenen Person bereitgestellten Informationen mit dem Verantwortlichen in Verbindung zu bringen, so verweist der Auftragsverarbeiter die betroffene Person an den Verantwortlichen. Der Auftragsverarbeiter leitet die Anfrage der betroffenen Person unverzüglich an den Verantwortlichen weiter. Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen

seiner Möglichkeiten und auf der Grundlage der Anweisungen des Verantwortlichen. Der Verantwortliche trägt alle zusätzlichen Kosten, die durch die in diesem Abschnitt beschriebene Unterstützung des Auftragsverarbeiters entstehen.

§ 7 Prüfungsverpflichtungen

(1) Der Auftragsverarbeiter ist verpflichtet, die Einhaltung der in diesem AV-Vertrag vereinbarten Verpflichtungen zu dokumentieren und dem Verantwortlichen auf Verlangen und auf Kosten des Verantwortlichen durch geeignete Methoden nachzuweisen, wobei der Verantwortliche eine solche Aufforderung nicht öfter als einmal pro Jahr aussprechen darf. Die Parteien vereinbaren, dass die Dokumentation und der Nachweis durch die Vorlage der folgenden Unterlagen und/oder Bescheinigungen erbracht werden kann:
   - Durchführung eines Selbstaudits
   - interne Compliance-Vorschriften einschließlich externer Nachweise für die Einhaltung dieser Vorschriften
   - Zertifizierungen zum Datenschutz und/oder zur lnformationssicherheit (z. B. ISO 27001)
   - gemäß Artikel 40 der Datenschutz-Grundverordnung genehmigte Verhaltenskodizes
   - Zertifizierungen gemäß Artikel 42 DSGVO.

(2) Soweit (i) der Verantwortliche nachweisen kann, dass die vom Auftragsverarbeiter gemäß Abschnitt 7.1 zur Verfügung gestellten Informationen nicht ausreichen, um den Verantwortlichen in die Lage zu versetzen, die gesetzlich vorgeschriebenen Datenschutz-Folgenabschätzungen durchzuführen, und (ii) der Auftragsverarbeiter nach der DSGVO verpflichtet ist, kann der Verantwortliche auf eigene Kosten nach angemessener und rechtzeitiger Vorankündigung, während der regulären Geschäftszeiten, ohne Unterbrechung des Geschäftsbetriebs des Auftragsverarbeiters und nicht öfter als einmal pro Jahr eine Vor-Ort-Inspektion des auftragsverarbeitungsrelevanten Geschäftsbetriebs des Auftragsverarbeiters durchführen oder durch einen qualifizierten Dritten durchführen lassen, der kein Wettbewerber des Auftragsverarbeiters sein darf. Der Auftragsverarbeiter kann verlangen, dass solche Vor-Ort-Prüfungen von (i) der vorherigen schriftlichen Bestätigung des Verantwortlichen, alle Kosten des Auftragsverarbeiters im Zusammenhang mit solchen Vor-Ort- Prüfungen zu tragen, und (ii) der Unterzeichnung einer Vertraulichkeitserklärung abhängig gemacht werden, die die Daten anderer Kunden des Auftragsverarbeiters und die Vertraulichkeit der vom Auftragsverarbeiters implementierten technischen und organisatorischen Maßnahmen und Sicherheitsvorkehrungen schützt.

§ 8 Unterauftragnehmer (Artikel 28 Absatz 3 Satz 2 lit. d DSGVO)

(1) Der Verantwortliche ist mit der Vergabe von Unteraufträgen an die zum Zeitpunkt der Unterzeichnung des AV-Vertrages eingesetzten und in der folgenden Tabelle aufgeführten Unterauftragnehmer einverstanden:

Zweck der Unterauftragsvergabe	**Unterauftragnehmer**	**Beschreibung**
Kundenbetreuung & Kundenbeziehungen	**VMRay Inc.** 51 Melcher Street, 7. Stock Boston, MA 02210, USA	Information über das Unternehmenskonto, Malware-Samples und Analyse-Informationen.

Hosting von Cloud- und Reputationsservice (Hosting-Standort entweder US oder EU, je nach Wahl des Unternehmens)	**Amazon Web Services EMEA Sàrl** 38, avenue John F. Kennedy, L-1855 Luxemburg	Informationen zum Unternehmenskonto, Malware-Samples und Analyse-Informationen.
Software zur Kundenbetreuung	**salesforce.com Deutschland GmbH** Erika-Mann-Straße 31-37, 80636 München, Deutschland	Kontoinformationen des Unternehmens und Informationen zur Malware-Analyse (falls dem Antrag des Kunden auf Unterstützung beigefügt).
Reputationsabfragen	**Bitdefender S.R.L.** Orhideea Towers Building 15A Orhideelor Avenue, 6th District, Bucharest, 060071 Rumänien	URLs, die in einigen Fällen personenbezogene Daten enthalten können, und IP-Adressen.
Reputationsabfragen	**Sophos Ltd.** The Pentagon, Abingdon Science Park, Abingdon OX14 3YP, UK	URLs, die in einigen Fällen personenbezogene Daten enthalten können, und IP-Adressen.
WHOIS-Abfragen	**Whois API, LLC** 340 S Lemon Ave, #1362 Walnut, CA 91789, USA	Domainnamen, die in einigen Fällen personenbezogene Daten enthalten können.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen vor dem Einsatz eines neuen Unterauftragnehmers oder dem Austausch eines der vorgenannten Unterauftragnehmer. Der Verantwortliche ist berechtigt, einer vom Auftragsverarbeiter mitgeteilten Änderung aus wichtigem Grund innerhalb von drei (3) Wochen nach Zugang der Änderungsmitteilung des Auftragsverarbeiters zu widersprechen (Artikel 28 Absatz 2 Satz 2 DSGVO). Widerspricht der Verantwortliche der Änderung nicht innerhalb dieser Frist, so gilt dies als Zustimmung des Verantwortlichen zu der Änderung. Liegt ein wichtiger Grund für einen solchen Widerspruch vor, und ist es den Parteien nicht gelungen, eine gütliche Einigung in dieser Angelegenheit zu erzielen, kann der Verantwortliche von seinem Kündigungsrecht gemäß der geltenden Handelsvereinbarung Gebrauch machen.

(3) Soweit der Auftragsverarbeiter Unteraufträge an Unterauftragnehmer vergibt, ist er verpflichtet, die datenschutzrechtlichen Verpflichtungen mit mindestens gleichwertiger Wirkung wie in diesem AV-Vertrag auf den Unterauftragnehmer zu erstrecken. Satz 1 gilt insbesondere, aber nicht abschließend, für die Anforderungen an die Vertraulichkeit und den Schutz von personenbezogenen Daten sowie die Datensicherheit, jeweils wie zwischen den Parteien vereinbart.

(4) Eine Beauftragung von Unterauftragnehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Artikel 44 ff. DSGVO erfüllt sind (z.B. Angemessenheitsbeschluss der EU-Kommission, EU-Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

(5) Der Vertrag mit dem Unterauftragnehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Artikel 28 Absatz 4 und Absatz 9 DSGVO).

(6) Die in diesem § 8 festgelegten Anforderungen für die Vergabe von Unterauftragen gelten nicht, wenn der Auftragsverarbeiter Unteraufträge für Nebenleistungen an Dritte vergibt; zu diesen Nebenleistungen gehören unter anderem die Beauftragung von externen Auftragnehmern, Post,

Versand- und Empfangsdienste sowie Wartungsdienste. Der Auftragsverarbeiter schließt diesen Dritten alle erforderlichen Vereinbarungen, um einen angemessenen Schutz der Daten zu gewährleisten.

§ 9 Schriftformgebot, Haftung, Rechtswahl

(1) Änderungen dieses AV-Vertrages sind nur dann gültig und verbindlich, wenn sie schriftlich oder in einem maschinenlesbaren Format (in Textform) erfolgen, und auch dann nur, wenn in einer solchen Änderung ausdrücklich darauf hingewiesen wird, dass sich diese Änderung auf die Bestimmungen dieses AV-Vertrages bezieht. Dies gilt auch für die Aufhebung oder Änderung dieses Schriftformerfordernisses.

(2) Die im Hauptvertrag enthaltenen Regelungen über die Haftung des Auftragsverarbeiters gelten auch für diesen Vertrag.

(3) Im Falle eines Konflikts und nur innerhalb des Geltungsbereichs dieses AV-Vertrages (nämlich des Datenschutzes) haben die Bestimmungen dieses AV-Vertrages Vorrang vor den Bestimmungen des Hauptvertrages.

(4) Sollten einzelne Bestimmungen dieses AV-Vertrages unwirksam oder undurchführbar sein, so wird die Wirksamkeit und Durchführbarkeit der übrigen Bestimmungen dieses AV-Vertrages nicht berührt. Gleiches gilt für Regelungslücken.

(5) Dieser AV-Vertrag unterliegt dem Recht der Bundesrepublik Deutschland.

Datum:	Datum:
Verantwortlicher	VMRay GmbH
_____	_____
Name: Position:	Name: Position:
	_____
	Name: Position: