Dienstspezifische Nutzungsbedingungen für SecOps

Diese dienstspezifischen Nutzungsbedingungen für SecOps sind Bestandteil der Vereinbarung, in der Google sich verpflichtet hat, dem Kunden SecOps-Dienste (wie unter https://cloud.google.com/terms/secops/services beschrieben) zur Verfügung zu stellen (die „Vereinbarung“). Wenn die Vereinbarung Sie dazu berechtigt, SecOps-Dienste im Rahmen eines Google Cloud-Partner- oder Resellerprogramms weiterzuverkaufen oder bereitzustellen, dann beziehen sich - außer im Abschnitt „Partnerspezifische Nutzungsbedingungen“- alle Verweise auf den “Kunden” in den dienstspezifischen Nutzungsbedingungen für SecOps auf Sie („Partner“ oder „Reseller“, wie in der Vereinbarung verwendet) und alle Verweise auf “Kundendaten” in den dienstspezifischen Nutzungsbedingungen für SecOps auf “Partnerdaten”. Wenn Sie die Dienste als Kunde eines nicht mit Google verbundenen Google Cloud-Resellers nutzen, gilt Abschnitt 9 (Kunden eines Resellers) der folgenden Dienstspezifische Nutzungsbedingungen für SecOps. Großgeschriebene Begriffe, die in den Dienstspezifische Nutzungsbedingungen für SecOps verwendet, aber nicht definiert werden, haben die ihnen in der Vereinbarung zugewiesene Bedeutung.

Allgemeine Dienstbedingungen

1. Daten

a. *Verbesserungen*. Um auf die sich ständig verändernde Bedrohungslage zu reagieren und aktuelle und hochmoderne Cybersicherheit zu bieten, verarbeiten wir im Rahmen der Bereitstellung der Dienste Kundendaten, um die Sicherheit, die Erkennung von Bedrohungen, die Prävention und die Reaktionsfähigkeiten dieser Dienste zu verbessern.

b. *Standort*. Der Kunde kann im Bestellformular oder, sofern von Google bereitgestellt, auf andere Weise auswählen, dass Kundendaten in einer bestimmten Region oder Multi-Region gespeichert werden sollen, wie auf der Seite „SecOps Services Locations“ („Auswahl des Datenstandorts“) beschrieben, und Google speichert diese Kundendaten im Ruhezustand nur in der ausgewählten Region/Multi-Region. Google kann diese Kundendaten innerhalb jeder anderen Region, die sich im Land der ausgewählten Region befindet, oder innerhalb des Landes oder der Länder der ausgewählten Multi-Region zu Sicherungs-, Verfügbarkeits-, Debugging-, Support-, Wartungs- oder Sicherheitszwecken replizieren. Die Dienste beschränken nicht die Standorte, von denen aus Kunden oder die Endnutzer des Kunden auf Kundendaten zugreifen oder an die sie Kundendaten umziehen dürfen. Zur Klarstellung: Der Begriff der Kundendaten umfasst keine Ressourcenkennungen, Attribute oder andere Datenlabels.

2. Allgemeine Softwarebedingungen. Die folgenden Nutzungsbedingungen gelten für die gesamte Software:

a. *Lizenz*. Google gewährt dem Kunden während der Laufzeit eine gebührenfreie (sofern von Google nicht anders angegeben), nicht ausschließliche, nicht unterlizenzierbare und nicht übertragbare Lizenz zur Vervielfältigung und Nutzung der vom Kunden bestellten Software auf Systemen, die dem Kunden gehören,

von ihm betrieben oder verwaltet werden oder in seinem Auftrag betrieben oder verwaltet werden, gemäß (i) der Vereinbarung und (ii) dem gegebenenfalls vereinbarten Nutzungsumfang ("Scope of Use"). Der Kunde kann seine Mitarbeiter, Vertreter und Subunternehmer sowie die seiner verbundenen Unternehmen (zusammenfassend „Software-Nutzer") zur Nutzung der Software gemäß diesem Abschnitt (Lizenz) autorisieren, solange der Kunde hierfür verantwortlich bleibt. Der Kunde darf eine angemessene Anzahl von Kopien der Software zu Sicherungs- und Archivierungszwecken anfertigen. Zur Klarstellung: Die Software stellt keine Dienste dar.

b. *Dokumentation*. Google kann eine Dokumentation bereitstellen, in der der bestimmungsgemäße Betrieb der Software beschrieben wird, einschließlich Nutzungsrichtlinien und Informationen dazu, ob und wie die Software Daten erfasst und verarbeitet. Der Kunde wird alle in der Dokumentation enthaltenen Einschränkungen hinsichtlich der Nutzung der Software einhalten.

c. *Einhaltung des Scope of Use*. Innerhalb von 30 Tagen nach einer zumutbaren schriftlichen Aufforderung durch Google wird der Kunde schriftlich und detailliert Auskunft über die Nutzung gemäß des jeweils anwendbaren Scope of Use geben, und zwar in Bezug auf jedes vom Kunden und seiner Softwarenutzer im angefragten Zeitraum verwendeten Softwareprodukt. Auf entsprechende Anfrage gewährt der Kunde angemessene Unterstützung und Zugriff auf Informationen, um die Richtigkeit der Auskunft des Kunden zu überprüfen.

d. *Sonstige Gewährleistungen und Einhaltung rechtlicher Vorschriften*. Jede Partei sichert zu und gewährleistet, dass sie alle für die Bereitstellung oder Nutzung der Software geltenden Gesetze und Vorschriften einhält.Der Kunde wird: (i) sicherstellen, dass die Nutzung der Software durch den Kunden und seine Software-Nutzer mit der Vereinbarung und den in der Vereinbarung enthaltenen Beschränkungen für die Nutzung der Dienste durch den Kunden übereinstimmt; (ii) wirtschaftlich angemessene Anstrengungen unternehmen, um jeden unbefugten Zugriff auf die Software oder deren unbefugte Nutzung zu verhindern und zu beenden; und (iii) Google schnellstmöglich über jeden unbefugten Zugriff auf die Software oder deren unbefugte Nutzung informieren, von dem der Kunde Kenntnis erlangt. Wenn die Software Open-Source- oder Drittanbieterkomponenten enthält, können diese Komponenten separaten Lizenzvereinbarungen unterliegen, die Google dem Kunden zur Verfügung stellen wird. Der Kunde ist allein verantwortlich für die Einhaltung der Bedingungen aller Drittanbieter, von denen der Kunde seine Workloads auf die Dienste migrieren möchte, und versichert und garantiert, dass diese Drittanbieter die Nutzung der Software zur Migration von Anwendungen aus diesen Quellen gestatten. Bei Beendigung oder Ablauf der Vereinbarung wird der Kunde die Nutzung der gesamten Software einstellen und diese aus seinen Systemen löschen.

3. Nutzungsbedingungen für Premium-Software. Die folgenden Nutzungsbedingungen gelten nur für Premium-Software:

a. *Einführung*. Google stellt bestimmte Software im Rahmen der Vereinbarung zur Verfügung, die in einem Bestellformular oder anderweitig von Google als „Premium-Software" („Premium-Software") bezeichnet wird. Der Kunde bezahlt für von ihm erworbene Premium-Software die anfallenden Gebühren, die im jeweiligen Bestellformular festgelegt sind. Bei Premium-Software handelt es sich um vertrauliche Informationen von Google.

b. *Softwaregewährleistung*. Google gewährleistet dem Kunden, dass Premium-Software ab Auslieferung ein Jahr in ihrer Funktionsweise im Wesentlichen der geltenden Dokumentation entspricht. Diese Gewährleistung gilt nicht, wenn (i) der Kunde Google über einen Mangel nicht innerhalb von 30 Tagen nach dessen Entdeckung informiert, (ii) der Kunde die Premium-Software ändert oder seine Nutzung gegen die

Vereinbarung verstößt oder (iii) der Mangel durch Hardware, Software, Dienste oder andere Angebote oder Materialien von Dritten verursacht wird, die jeweils nicht von Google bereitgestellt werden.

Falls Google diese Gewährleistung verletzt, wird Google nach eigenem Ermessen die betroffene Premium-Software ohne Zusatzkosten reparieren oder ersetzen. Falls Google eine Reparatur oder einen Ersatz nicht für wirtschaftlich vernünftig hält, informiert Google den Kunden darüber und (A) der Kunde beendet sofort die Nutzung der betroffenen Premium-Software und (B) Google erstattet etwaige vorab bezahlte Beträge für die betroffene Premium-Software oder schreibt sie gut und dem Kunden werden alle noch geltenden Zahlungsverpflichtungen für die zukünftige Nutzung der betroffenen Premium-Software erlassen. Vorbehaltlich der Kündigungsrechte der Parteien enthält dieser Abschnitt (Softwaregewährleistung) eine abschließende Regelung der dem Kunden im Falle einer Verletzung der in diesem Abschnitt (Softwaregewährleistung) geregelten Gewährleistung zustehenden Rechte.

c. *Haftungsfreistellung in Bezug auf Software*. Die in der Vereinbarung vereinbarten Freistellungsverpflichtungen von Google in Bezug auf behauptete Verletzungen von Rechten an geistigem Eigentum Dritter finden auch auf die Premium-Software Anwendung. Die in der Vereinbarung vereinbarten Freistellungsverpflichtungen des Kunden in Bezug auf die Nutzung der Services durch den Kunden finden auch Anwendung auf die Nutzung der Premium Software. Zusätzlich zu anderen Haftungsausschlüssen in der Vereinbarung bestehen die Freistellungsverpflichtungen von Google nicht, soweit die behaupteten Ansprüche Dritter beruhen auf Änderungen an der Premium-Software, die nicht von Google vorgenommen wurden, oder auf der Nutzung von Versionen der Premium-Software, die von Google nicht mehr unterstützt werden.

d. *Technischer Support*. Sofern von Google nicht anders angegeben, wird Google TSD für Premium-Software gegen eine zusätzliche Gebühr und wie in den TSD-Richtlinien festgelegt bereitstellen.

e. *Compliance*. Premium-Software kann, wie in der jeweiligen Dokumentation beschrieben, Messdaten an Google übermitteln, die verständigerweise zur Überprüfung der Einhaltung des Scope of Use erforderlich sind. Der Kunde darf die Übermittlung dieser Messdaten nicht deaktivieren oder stören.

f. *Updates und Maintenance*. Während der Laufzeit wird Google dem Kunden alle aktuellen Versionen, Updates und Upgrades der Premium-Software, sobald diese allgemein verfügbar sind, gemäß der Dokumentation zur Verfügung stellen. Sofern in der Dokumentation für die jeweilige Softwarekomponente nicht anders angegeben, unterstützt Google die jeweils aktuelle Version der Premium-Software sowie die zwei vorangegangenen Versionen, einschließlich der angemessenen Bereitstellung von bug fixes und Sicherheitspatches. Google kann die Unterstützung für jede Premium-Software mit einer Frist von einem Jahr einstellen. Hiervon unberührt bleibt das Recht Googles, die Unterstützung für eine Version einzustellen und ein Upgrade auf eine unterstützte Version verlangen, um ein erhebliches Sicherheitsrisiko zu beheben oder wenn dies vernünftigerweise erforderlich ist, um eine Verletzung von Rechten zu vermeiden oder um geltendes Recht einzuhalten.

4. Bedingungen für Pre-GA-Angebote. Google kann dem Kunden Funktionen, Dienste oder Software vor der allgemeinen Verfügbarkeit zur Verfügung stellen, die entweder noch nicht unter https://cloud.google.com/terms/secops/services aufgeführt oder in der zugehörigen Dokumentation oder den zugehörigen Materialien als „Early Access“, „Alpha“, „Beta“, „Vorabversion“, „Experimentell“ oder mit einer ähnlichen Bezeichnung gekennzeichnet sind (zusammenfassend als „Pre-GA-Angebote“ bezeichnet). Pre-GA-Angebote sind weder Dienste noch Software unter der Vereinbarung. Die Parteien ergänzen Ihre Vereinbarung unter dieser Ziffer 4 jedoch dahin, dass auf Pre-GA-Angebote die Bestimmungen der Vereinbarung für Dienste oder, soweit zutreffend, für Software entsprechend anzuwenden sein sollen.

Der Kunde hat die Möglichkeit, Feedback und Vorschläge zu den Pre-GA-Angeboten an Google zu senden. Wenn der Kunde Feedback gibt, können Google und dessen verbundenes Unternehmen dieses Feedback uneingeschränkt und ohne Verpflichtungen gegenüber dem Kunden nutzen.

PRE-GA-ANGEBOTE WERDEN „WIE BESEHEN“ OHNE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GEWÄHRLEISTUNGEN ODER ZUSICHERUNGEN JEGLICHER ART BEREITGESTELLT. Pre-GA-Angebote (a) können jederzeit ohne vorherige Ankündigung gegenüber dem Kunden geändert, ausgesetzt oder eingestellt werden und (b) fallen nicht unter eine SLA oder eine Freistellungsverpflichtung von Google. Sofern nicht ausdrücklich in einer schriftlichen Mitteilung oder in der Dokumentation zu einem bestimmten Pre-GA-Angebot anders angegeben, (i) sind Pre-GA-Angebote möglicherweise nicht durch TSS abgedeckt, (ii) gilt der Zusatz zur Cloud-Datenverarbeitung nicht für Pre-GA-Angebote, und der Kunde sollte Pre-GA-Angebote nicht zur Verarbeitung personenbezogener Daten oder anderer Daten verwenden, die gesetzlichen oder behördlichen Compliance-Anforderungen unterliegen, und (iii) gelten die in diesen dienstspezifischen Bedingungen festgelegten Verpflichtungen von Google hinsichtlich des Speicherorts der Daten nicht für Pre-GA-Angebote. In Bezug auf Pre-GA-Angebote ist - im maximal zulässigem Umfang des anwendbaren Rechts - die Haftung von Google und seinen Lieferanten beschränkt auf den geringeren Betrag (A) der in der Vereinbarung vereinbarten Haftungshöchstsumme oder (B) 25.000 US-Dollar. Die vorstehende Bestimmung hat keinen Einfluss auf die übrigen Bestimmungen der Vereinbarung in Bezug auf die Haftung (einschließlich spezifischer Ausschlüsse von Haftungsbeschränkungen). Der Zugriff des Kunden auf Pre-GA-Angebote und deren Nutzung unterliegen dem vereinbarten Scope of Use. Jede Partei kann die Nutzung eines Pre-GA-Angebots durch den Kunden jederzeit durch schriftliche Mitteilung an die andere Partei kündigen. Bestimmte Pre-GA-Angebote können zusätzlichen Bedingungen unterliegen, die nachstehend aufgeführt sind.

5. Benchmarking. Der Kunde kann die Dienste Benchmark-Tests (jeweils ein „Test“) unterziehen. Die Ergebnisse solcher Tests darf der Kunde nur dann veröffentlichen, wenn er (a) vorab eine schriftliche Einwilligung von Google einholt, (b) Google alle notwendigen Informationen zur Reproduktion des Tests zukommen lässt und (c) Google erlaubt, die öffentlich verfügbaren Produkte und Dienste des Kunden Benchmark-Tests zu unterziehen und die Ergebnisse solcher Tests offenzulegen. Ungeachtet des Vorstehenden darf der Kunde ohne die vorherige schriftliche Einwilligung von Google keine der folgenden Handlungen für einen Anbieter von Hyperscale-Public-Cloud-Diensten vornehmen: (i) Durchführung eines Tests der Dienste (direkt oder durch einen Dritten) oder (ii) Offenlegung der Ergebnisse eines solchen Tests.

6. Trials. Bestimmte Dienste können dem Kunden im Rahmen einer Testversion mit einem Testkonto („Trial Account“) zur Verfügung gestellt werden. Die Rahmenbedingungen (engl. “parameters“) einer Testversion, einschließlich eines gegebenenfalls vereinbarten Scope of Use, können von Google gegenüber dem Kunden im Bestellformular, der Dokumentation, per E-Mail oder über einen anderen Kommunikationskanal festgelegt werden. Durch die Nutzung der Testversion akzeptiert der Kunde die parameters. Wenn die Testversion abläuft oder beendet wird, hat der Kunde über den Trial Account keinen Zugriff mehr auf die Dienste. Alle Kundendaten in den Diensten werden gelöscht, außer der Kunde bestellt den Dienst vor Ablauf des Testzeitraums.

7. Generative KI-Funktionen.

a. *Haftungsausschluss.* **Generative KI-Funktionen nutzen neue Technologien, können fehlerhafte oder anstößige Ausgaben (engl. “Output”) erstellen und sind nicht dazu geeignet oder bestimmt, die behördlichen, rechtlichen oder sonstigen Verpflichtungen des Kunden zu erfüllen. Der Kunde ist sich bewusst, dass eine generative KI-Funktion in manchen Fällen denselben oder einen ähnlichen Output für mehrere Kunden erzeugen kann.**

b. *Einschränkung der Nutzung von Kundendaten für Trainingszwecke*. Sofern der Kunde nicht zuvor eine Genehmigung oder Anweisung dazu erteilt hat, nutzt Google keine Kundendaten für das Training oder das Finetuning von Modellen für generative KI / maschinelles Lernen.

c. *Richtlinie zur verbotenen Nutzung*. Für die Zwecke der Bereitstellung generativer KI-Funktionen ergänzt die jeweils aktuelle Fassung der Richtlinie zur verbotenen Nutzung unter https://policies.google.com/terms/generative-ai/use-policy die AUP-Richtlinie.

d. *Nutzung zu Wettbewerbszwecken*. Der Kunde wird die generativen KI-Funktionen oder deren Ergebnisse nicht zur Entwicklung eines ähnlichen oder konkurrierenden Produkts oder einer ähnlichen oder konkurrierenden Dienstleistung nutzen und dies auch Endnutzern nicht gestatten. Google kann die Nutzung generativer KI-Funktionen durch den Kunden bei Verdacht auf einen Verstoß gegen den vorstehenden Satz unverzüglich aussetzen oder beenden.

e. *Modelleinschränkungen*. Der Kunde wird die Ausgabe von generativen KI-Funktionen nicht verwenden und Endnutzern nicht gestatten, diese zu verwenden, um: (i) die Verwendung eines Google-Modells direkt oder indirekt zu ersetzen, auszutauschen oder zu umgehen oder (ii) Modelle zu erstellen oder zu verbessern, die einem Google-Modell ähnlich sind.

f. *Kein Reverse Engineering*. Der Kunde wird keine Komponenten der generativen KI-Funktionen, der Software oder ihrer Modelle zurückentwickeln (Reverse Engineering) oder extrahieren (z. B. durch Verwendung von Eingabeaufforderungen zum Auffinden von Trainingsdaten) und wird dies auch Endnutzern nicht gestatten. Google kann die Nutzung der generativen KI-Funktionen durch den Kunden bei Verdacht auf einen Verstoß gegen den vorstehenden Satz unverzüglich aussetzen oder beenden.

Der Kunde wird keine Komponenten der generativen KI-Funktionen, der Software oder ihrer Modelle zurückentwickeln (Reverse Engineering) oder extrahieren (z. B. durch Verwendung von Prompts zum Auffinden von Trainingsdaten) und wird dies auch Endnutzern nicht gestatten. Google kann die Nutzung der generativen KI-Funktionen durch den Kunden bei Verdacht auf einen Verstoß gegen den vorstehenden Satz unverzüglich aussetzen oder beenden.

g. *Altersbeschränkung*. Der Kunde wird keine generative KI-Funktion als Teil einer Website oder eines anderen Online-Dienstes verwenden, der sich an Personen unter 18 Jahren richtet oder von diesen wahrscheinlich genutzt wird, und wird dies auch Endnutzern nicht gestatten.

h. *Einschränkungen im Gesundheitswesen*. Der Kunde wird generative KI-Funktionen nicht für klinische Zwecke, als Ersatz für fachliche medizinische Ratschläge oder in irgendeiner Weise nutzen, die von einer entsprechenden Regulierungsbehörde beaufsichtigt wird oder deren Genehmigung erfordert, und er wird dies auch Endnutzern nicht gestatten. Die Nutzung für nicht klinische Forschung, Terminplanung oder andere administrative Aufgaben ist nicht eingeschränkt.

i. *Mutmaßliche Verstöße*. Google kann die Nutzung von generativen KI-Funktionen durch den Kunden bei einem mutmaßlichen Verstoß gegen die oben genannten Absätze (c) oder (d) sofort aussetzen oder beenden.

j. *Einschränkungen*. Die in den oben genannten Absätzen (g) und (h) aufgeführten Einschränkungen gelten als „Einschränkungen“ oder „Nutzungseinschränkungen“ im Sinne der jeweils anwendbaren Vereinbarung.

8. Support. Wenn der Kunde kein bestehender Kunde der Google Cloud Platform ist, gelten die folgenden Bedingungen: Um auf die technischen Support-Services zugreifen zu können, muss sich der Kunde bei der Google Cloud Platform-Adminkonsole („GCP-Adminkonsole“) anmelden und die Nutzungsbedingungen der Google Cloud Platform unter https://cloud.google.com/terms („GCP-Nutzungsbedingungen“) akzeptieren. Der

Zugriff auf die GCP-Adminkonsole bietet dem Administrator des Kunden die Möglichkeit (aber keine Verpflichtung), bestimmte Google Cloud Platform-Dienste (beschrieben unter https://cloud.google.com/terms/services(die „GCP-Dienste“)) zu nutzen. Zur Klarstellung: Der Kunde ist nicht verpflichtet, GCP-Dienste zu erwerben oder zu nutzen, um über die GCP-Adminkonsole auf die technischen Supportleistungen zuzugreifen oder diese zu nutzen, und der Kunde ist nicht an die GCP-Nutzungsbedingungen gebunden, sofern er auf die GCP-Adminkonsole nur zugreift, um technische Supportleistungen in Anspruch zu nehmen.

9. Kunden eines Resellers. Dieser Abschnitt 9 (Kunden eines Resellers) kommt nur zur Anwendung, wenn (i) der Kunde SecOps-Dienste bei einem Reseller im Rahmen einer Reseller-Vereinbarung bestellt (diese Dienste werden dann als „über einen Reseller erworbene Dienste“ bezeichnet) und (ii) der Kunde eine direkte Vereinbarung mit Google über die Bereitstellung dieser über einen Reseller erworbenen Dienste hat.

a. *Anwendbare Nutzungsbedingungen*. Für die Zwecke der über einen Reseller erworbenen Dienste gilt Folgendes:

   i. Abschnitte der Vereinbarung, die den Titel „Zahlungsbedingungen“ tragen, finden keine Anwendung. Dies gilt auch für andere Bestimmungen in der Vereinbarung (einschließlich dieser dienstspezifischen Nutzungsbedingungen für SecOps) mit Bezug zu Abrechnung, Rechnungsstellung oder Bezahlung.

   ii. Es gelten die Reseller-Gebühren und diese sind vom Kunden direkt an den Reseller zu zahlen. Die Preise für die über einen Reseller erworbenen Dienste werden ausschließlich zwischen Reseller und Kunde festgelegt.

   iii. Google stellt dem Kunden die in der Reseller-Bestellung beschriebenen Reseller-Dienste in dem Umfang zur Verfügung, in dem eine gültige und verbindliche Bestellung für diese Dienste zwischen Google und dem Reseller vorliegt. Ungeachtet des Vorstehenden kann der Kunde für über einen Reseller erworbene Mandiant Consulting-Dienste verpflichtet sein, ein Bestellformular direkt mit Google abzuschließen.

   iv. Etwaige SLA-Gutschriften oder Rückerstattungen gemäß dieser Vereinbarung erhält der Kunde ausschließlich vom Reseller (und der Kunde muss den Reseller benachrichtigen, wenn Google ein SLA nicht einhält).

   v. Ungeachtet der Supportverpflichtungen von Google gemäß den TSD-Richtlinien, schuldet Google dem Kunden keinen Support, es sei denn, (i) der Kunde bestellt TSD direkt bei Google oder (ii) der Reseller bestellt TSD bei Google im Namen des Kunden, und diese TSD-Berechtigung erfordert, dass Google TSD direkt gegenüber dem Kunden erbringt. Alle anderen etwaigen Supportleistungen werden dem Kunden vom Reseller in Übereinstimmung mit der Reseller-Vereinbarung und nach Maßgabe des Abschnitts 9(e) (Technischer Support durch den Reseller) erbracht.

   vi. Der Kunde nimmt zur Kenntnis, dass der Zugang zu den Diensten gesperrt werden kann, wenn der Reseller oder der Kunde zu irgendeinem Zeitpunkt kein mit dem Kundenkonto verknüpftes Abrechnungskonto unterhält.

   vii. Im Falle der Beendigung der Vereinbarung sendet Google dem Reseller (und nicht dem Kunden) die Schlussrechnung (falls zutreffend) für die Zahlungsverpflichtungen im Zusammenhang mit den über den Reseller erworbenen Diensten. Der Kunde benachrichtigt (i) den Reseller über jegliche Beendigung der Vereinbarung und (ii) Google über jegliche Beendigung der Reseller-Vereinbarung.

   viii. Jegliche Verlängerung (engl. “Renewal”) der über einen Reseller erworbenen Dienste und/oder einer Reseller-Bestellung erfolgt gemäß der Vereinbarung zwischen dem Kunden und dem Reseller.

ix. Wenn der Reseller eine unwidersprochene Rechnung von Google für über einen Reseller erworbene Dienste nicht bezahlt, weil der Kunde den Reseller nicht bezahlt hat, kann Google den Zugriff des Kunden auf die Dienste sperren.

x. Soweit sich Kundendaten in Ressourcen in der Organisationssphäre des Resellers befinden, gilt ungeachtet anderslautender Bestimmungen in dieser Vereinbarung (einschließlich des Zusatzes zur Verarbeitung von Cloud-Daten) Folgendes:

(A) Der Zusatz zur Verarbeitung von Cloud-Daten gilt nicht für die Verarbeitung und Sicherheit solcher Kundendaten.

(B) Google wird auf diese Kundendaten nur in Übereinstimmung mit der separaten Vereinbarung zwischen Google und dem Reseller zugreifen, sie nutzen und anderweitig verarbeiten (einschließlich der jeweils geltenden Bedingungen, die die Datenverarbeitung und Sicherheit von „Partnerdaten“ gemäß der Definition in dieser separaten Vereinbarung beschreiben) und wird auf diese Kundendaten nicht zu anderen Zwecken zugreifen, sie nutzen oder verarbeiten.

(C) Die Einwilligungen und Mitteilungen, für die der Kunde gemäß den Abschnitten der Vereinbarung mit dem Titel „Datenschutz“ oder „Einwilligungen“ verantwortlich ist, müssen auch den Zugriff auf, die Speicherung und die Verarbeitung von Kundendaten wie in Absatz (B) oben beschrieben erlauben.

xi. Für die Abrechnung ist es erforderlich, bestimmte SecOps-Dienste mit dem Abrechnungskonto des Resellers zu verknüpfen. Der Kunde nimmt das Folgende zur Kenntnis und ist damit einverstanden: (A) Bei Beendigung oder Ablauf der separaten Vereinbarung zwischen Google und dem Reseller oder der Reseller-Vereinbarung mit dem Kunden wird diese Verknüpfung aufgelöst. (B) Wenn vom Kunden genutzte Dienste nicht mehr mit dem Abrechnungskonto des Resellers verknüpft sind, gilt: (x) Diese Dienste gelten dann nicht mehr als über einen Reseller erworbene Dienste (und unterliegen damit nicht diesem Abschnitt 9 „Kunden eines Resellers“). (y) Diese Dienste gelten dann als direkt bei Google bestellte Dienste, wodurch der Kunde direkt an Google Gebühren für diese Dienste gemäß den Bedingungen dieser Vereinbarung zahlen muss, ungeachtet anderslautender Vereinbarungen mit dem Reseller (einschließlich solcher über die zwischen Reseller und Kunde vereinbarten Gebühren). Informationen dazu, welche SecOps-Dienste verknüpft werden müssen, erhält der Kunde vom Reseller.

xii. Der „Zusatz zur Verarbeitung von Cloud-Daten“ bezeichnet in dieser Vereinbarung die jeweils aktuellen Datenverarbeitungs- und Sicherheitsbestimmungen für Kundendaten, die (i) in Ressourcen in der Organisationssphäre des Kunden (und nicht des Resellers) vearbeitet werden oder (ii) sich auf Mandiant Consulting Resold Services oder Mandiant Managed Resold Services beziehen, wie unter https://cloud.google.com/terms/data-processing-addendum/ beschrieben.

xiii. „Laufzeit der Bestellung“ bezeichnet in dieser Vereinbarung den Zeitraum, der mit dem Startdatum der Dienste oder dem Verlängerungsdatum (je nach Anwendbarkeit) für die über einen Reseller erworbenen Dienste beginnt und bis zum Ablauf oder zur Beendigung der jeweiligen Reseller-Bestellung andauert.

xiv. Das „Startdatum der Dienste“ bezeichnet in dieser Vereinbarung entweder das in der Reseller-Bestellung angegebene Startdatum oder, falls in der Reseller-Bestellung kein Datum angegeben ist, das Datum, ab dem Google dem Kunden die über einen Reseller erworbenen Dienste zur Verfügung stellt.

b. Haftungsbeschränkung. Für die Zwecke des Abschnitts „Beschränkung der Haftungshöhe“ der Vereinbarung meinen „Gebühren“ die „Reseller-Gebühren“, wenn das Ereignis, das zu einer Haftung führt, ein Verstoß gegen diese Vereinbarung ist oder anderweitig im Zusammenhang mit den über einen Reseller erworbenen Diensten entsteht. Wenn der Kunde oder Google einen Anspruch gemäß der Vereinbarung geltend macht, wird der Kunde

zum Zwecke der Festlegung der Haftungsobergrenze gemäß des Abschnitts „Beschränkung der Haftungshöhe“ der Vereinbarung auf Anfrage von Google (i) Google unverzüglich den Betrag aller im Rahmen der Reseller-Vereinbarung gezahlten oder zu zahlenden Reseller-Gebühren offenlegen, (ii) der Offenlegung dieses Betrags durch den Reseller gegenüber Google zustimmen, ungeachtet der Vertraulichkeitsverpflichtungen des Resellers gemäß der Reseller-Vereinbarung, und (iii) alle erforderlichen Zustimmungen einholen, um die Offenlegung durch den Kunden oder den Reseller gemäß diesem Abschnitt 9(b) (Haftungsbeschränkung) zu ermöglichen. Vorbehaltlich des Abschnitts „Unbegrenzte Haftung“ der Vereinbarung haftet Google nicht für Schäden im Rahmen dieser Vereinbarung, soweit der Kunde Schadensersatzansprüche in Bezug auf dasselbe Ereignis oder dieselbe Reihe von Ereignissen gegenüber dem Reseller geltend gemacht hat.

c. *Weitergabe vertraulicher Informationen*. Google ist befugt, vertrauliche Kundeninformationen gemäß dem Abschnitt „Vertraulichkeit“ oder „Vertrauliche Informationen“ der Vereinbarung Resellern als Delegierte von Google offenzulegen.

d. *Beziehung zwischen Reseller und Kunde*. Der Reseller kann nach Ermessen des Kunden auf das Konto des Kunden zugreifen. Im Verhältnis zwischen Google und dem Kunden ist der Kunde allein verantwortlich für (i) jeden Zugriff des Resellers auf das Konto des Kunden; (ii) die Festlegung aller Rechte und Pflichten zwischen dem Reseller und dem Kunden in Bezug auf die über den Reseller erworbene Dienste in der Reseller-Vereinbarung und (iii) die Überprüfung, ob die Daten, die der Kunde oder die Endnutzer Google über durch Reseller erworbene Dienste (außer über Mandiant erworbene Consulting Services oder Managed Services) im Rahmen des Kontos zur Verfügung stellen, und die Daten, die der Kunde oder die Endnutzer durch ihre Nutzung der über einen Reseller erworbenen Dienste von diesen Daten ableiten, in Ressourcen in der Organisationssphäre des Kunden oder des Resellers fallen. Google übernimmt keine Haftung für (x) die Sperrung oder Kündigung des Zugangs des Kunden zu den Diensten durch einen Reseller; (y) den Zugriff auf und die Sichtbarkeit des Kundenkontos und der abrechnungsbezogenen Metadaten des Kundenkontos; oder (z) das Anbieten oder Bereitstellen von Produkten oder Dienstleistungen des Resellers oder Dritter.

e. *Technischer Support durch den Reseller.* Der Kunde nimmt zur Kenntnis und ist damit einverstanden, dass der Reseller personenbezogene Daten des Kunden und von Endnutzern gegenüber Google offenlegen kann. Das gilt insofern, als die Offenlegung verständigerweise erforderlich ist, damit der Reseller Supportanfragen bearbeiten kann, die der Kunde an oder über den Reseller eskaliert.

f. *Fortbestand*. Die folgenden Absätze dieses Abschnitts 9 (Kunden eines Resellers) bestehen über den Ablauf oder die Beendigung der Vereinbarung hinaus fort: Abschnitte 9(a)(vii) (Beendigung der Reseller-Vereinbarung), 9(b) (Haftungsbeschränkung), 9(c) (Weitergabe vertraulicher Informationen) und 9(d) (Beziehung zwischen Reseller und Kunde).

10. Weitere Definitionen.

„Dokumentation“ bezeichnet die Google-Dokumentation (die von Zeit zu Zeit aktualisiert werden kann) in der Form, in der sie dem Kunden von Google zur Nutzung mit den entsprechenden Diensten zur Verfügung gestellt wird. Dies wird unten in den Nutzungsbedingungen der einzelnen SecOps-Dienste genauer definiert.

„*Generative KI-Funktion(en)*“ bezeichnet jegliche auf generativer KI basierende Funktionen eines Dienstes.

„*Google-Modelle*“ bezeichnet ein von Google trainiertes und nicht als Open Source oder mit einer anderen Lizenz veröffentlichtes offenes Modell.

„*Multi-Region*“ bezeichnet eine festgelegte Gruppe von Regionen.

„*Reseller*“ meint den von Google autorisierten, aber nicht mit Google verbundenen Reseller, von dem der Kunde gegebenenfalls die Dienste erwirbt.

„*Reseller-Vereinbarung*“ bezeichnet die gegebenenfalls zwischen dem Kunden und dem Reseller abgeschlossene gesonderte Vereinbarung bezüglich der Dienste. Die etwaige Reseller-Vereinbarung besteht unabhängig von der Vereinbarung und unterliegt nicht den Regelungen der Vereinbarung.

„*Reseller-Gebühren*“ bezeichnet die etwaigen, in der Reseller-Vereinbarung vereinbarten Gebühren für die Nutzung oder Bestellung, zuzüglich jeglicher anfallender Steuern.

„*Reseller-Bestellung*“ bezeichnet ein gegebenenfalls vom Reseller erstelltes und vom Kunden und dem Reseller unterzeichnetes Bestellformular, in dem die vom Kunden beim Reseller bestellten Dienste spezifiziert werden.

„*Region*“ bezeichnet eine Region, aus der eine bestimmte Dienstleistung angeboten wird, wie auf der Seite „Standorte der SecOps-Dienstleistungen“ angegeben.

„*Scope of Use*“ bezeichnet alle von Google vorgegebenen Beschränkungen hinsichtlich der Installation oder Nutzung von Diensten oder Software.

„*Seite der Standorte der SecOps-Dienste*“ bedeutet https://cloud.google.com/terms/secops/data-residency.

In diesen dienstspezifischen Nutzungsbedingungen hat „Zusatz zur Verarbeitung von Cloud-Daten“ (zuvor als „Bedingungen zu Datenverarbeitung und Datensicherheit“ bezeichnet) die in der Vereinbarung beschriebene Bedeutung. Falls keine solche Bedeutung beschrieben ist, bezeichnet dieser Begriff die jeweils aktuellen Datenverarbeitungs- und Sicherheitsbestimmungen für Kundendaten unter https://cloud.google.com/terms/data-processing-addendum.

Wenn der Kunde SecOps-Dienste bei einem Reseller im Rahmen einer Reseller-Vereinbarung bestellt, bezeichnet „Bestellformular“ in diesen dienstspezifischen Nutzungsbedingungen für SecOps auf ein Bestellformular, eine Leistungsbeschreibung oder ein anderes Bestelldokument, das von Google ausgestellt und vom Reseller und Google in Bezug auf die über den Reseller erworbenen Dienste unterzeichnet wurde.

Nutzungsbedingungen

Die folgenden Nutzungsbedingungen gelten nur für die jeweils im Titel des Unterabschnitts genannten Dienste.

1. Google Security Operations (Google SecOps – SIEM / Google SecOps – SOAR)

a. Dienstmodelle. Google Security Operations ist in den folgenden Dienstmodellen verfügbar, wie im jeweiligen Bestellformular konkretisiert:

i. *Data Ingestion (Log Ingest)*. Kunden bezahlen einen Pauschalpreis für die Datenaufnahme bis zur Datenobergrenze. Für dieses Dienstmodell gelten die folgenden Nutzungsbedingungen:

A. *Kontingentüberschreitungen*. Im Bestellformular ist die Datenobergrenze des Kunden als Anzahl der gekauften Einheiten angegeben. Falls der Kunde mehr als die gekauften Einheiten verbraucht (wie Google nach eigenem Ermessen feststellt), stellt Google dem Kunden nachträglich zum Monatsende die zusätzlich verbrauchten Einheiten in Rechnung, Sofern nichts anderes vereinbart ist, erfolgt dies anteilig zum monatlichen Preis, abzüglich im Bestellformular festgelegter Rabatte. Der Kunde bezahlt die Rechnung bis zum Fälligkeitsdatum der Zahlung. Falls der Kunde die Rechnung nicht innerhalb von dreißig (30) Tagen nach dem Fälligkeitsdatum bezahlt, kann Google das jeweilige Bestellformular nach schriftliche Benachrichtigung des Kunden kündigen.

ii. *Covered Personnel*. Kunden wird pro abgedecktem Mitarbeiter ein Pauschalpreis in Rechnung gestellt. Für dieses Dienstmodell gelten die folgenden Nutzungsbedingungen:

A. *Dateneinschränkungen*. Google Security Operations darf nur für Netzwerktelemetrie und Drittanbietertelemetrie genutzt werden. Der Kunde stimmt zu, Google Security Operations keine Daten bereitzustellen, die nicht Netzwerk- oder Drittanbieter-Telemetriedaten sind. Weiterhin erklärt sich der Kunde bereit, mit Google zusammenzuarbeiten, um Kundendaten zu filtern, die keine Netzwerk- oder Drittanbieter-Telemetriedaten darstellen.

B. *Kontingentüberschreitungen*. Im Bestellformular ist die Anzahl der abgedeckten Mitarbeiter als Anzahl der gekauften Einheiten angegeben. Wird die Anzahl der im Bestellformular festgelegten abgedeckten Mitarbeiter um zehn Prozent (10 %) oder mehr überschritten, steigen die vom Kunden zu zahlenden Gebühren während der Laufzeit der Bestellung proportional.

C. *Compliance*. Innerhalb von 30 Tagen nach einer zumutbaren schriftlichen Aufforderung durch Google stellt der Kunde eine Dokumentation zur Verfügung, die belegt, dass die Anzahl der abgedeckten Mitarbeiter, die Google Security Operations Kundendaten bereitstellen, die im Bestellformular angegebene Anzahl der Einheiten nicht um zehn Prozent (10 %) überschreitet.

b. Dienstsperrung. Google kann den Zugriff des Kunden auf Google Security Operations sperren, wenn dieser sich nicht an die in Unterabschnitt 1(a)(ii)(A) dieser Nutzungsbedingungen für Google Security Operations festgelegten Dateneinschränkungen hält und dieser Verstoß nach einer Mitteilung durch Google während der Mitteilungsfrist für Dateneinschränkungen nicht beseitigt wurde. Wenn Google den Zugriff des Kunden auf Google Security Operations gemäß diesem Unterabschnitt sperrt, (i) informiert Google den Kunden unverzüglich über die Sperrung, soweit dies rechtlich zulässig ist, und (ii) beschränkt die Sperrung auf den geringstmöglichen Umfang und die kürzeste Dauer, die zur Behebung des Grundes für die Sperrung erforderlich sind.

c. Datenzeitraum. Vorbehaltlich und in Übereinstimmung mit dem Zusatz zur Datenverarbeitung in der Cloud (i) bewahrt Google die Kundendaten während des Datenzeitraums in Google Security Operations auf, solange der Kunde über ein aktives Abonnement verfügt, und (ii) weist der Kunde Google an, die Kundendaten löschen zu dürfen, (A) im Falle der Kündigung oder des Ablaufs des Abonnements des Kunden (auch wenn der Datenzeitraum über diese Laufzeit hinausgeht) und (b) wenn der Datenzeitraum überschritten ist.

d. Drittanbieter- und ergänzende Bedingungen.

i. *Angebote von Drittanbietern*. Der Kunde muss sich den Zugang zu allen Angeboten von Drittanbietern vom jeweiligen Anbieter (einem „Drittanbieter“) verschaffen. Soweit der Kunde einem Drittanbieterangebot oder Drittanbieter Zugriff auf das Kundenkonto gewährt, erklärt sich der Kunde ausdrücklich damit einverstanden und weist Google an, dem Drittanbieter solcher Drittanbieterangebote den Zugriff auf Kundendaten zu gestatten, der für die Interaktion mit Google Security Operations erforderlich ist, einschließlich des Kopierens von Kundendaten in oder aus Google Security Operations. Zur Klarstellung: Drittanbieter sind keine Unterauftragsverarbeiter (im Sinne des Cloud-Datenverarbeitungszusatzes).

A. *Haftungsausschlüsse*. Die Art und Weise, wie Drittanbietern und ihre Angebote Kundendaten übermitteln, nutzen, speichern und offenlegen, unterliegen ausschließlich den Richtlinien dieser Drittanbieter bzw. Drittanbieterangebote. Soweit nach anwendbarem Recht zulässig, schließt Google für Folgendes jegliche Haftung und Verantwortung aus:

1. Nutzung eines Angebots von Drittanbietern durch den Kunden, einschließlich Schäden oder Verlusten, die durch oder im Zusammenhang mit der Nutzung oder Abhängigkeit von einem solchen Angebot von Drittanbietern entstanden oder angeblich entstanden sind, Google-fremde Integrationen der Dienste in Angebote von Drittanbietern, Maßnahmen oder Auswirkungen von Maßnahmen, die Google mit Genehmigung des Kunden im Hinblick auf Angebote von Drittanbietern ergreift, sowie Zugriff auf und Nutzung von Kundendaten durch einen Drittanbieter,

2. Datenschutzpraktiken oder andere Maßnahmen eines Drittanbieters oder von Drittanbieterangeboten;

3. Richtigkeit, Verfügbarkeit oder Zuverlässigkeit von Daten, Informationen, Inhalten, Diensten, Beratungen oder Aussagen, die im Zusammenhang mit einem Angebot von Drittanbietern verfügbar gemacht werden.

B. *Zusicherungen und Gewährleistungen*. Der Kunde sichert zu und gewährleistet, dass keine Bestimmung der Vereinbarung und keine Nutzung der Google Security Operations durch den Kunden gegen Vereinbarungen oder Bedingungen mit Dritten verstößt, denen der Kunde unterliegt.

ii. *Looker und BigQuery*. Google nutzt Looker und BigQuery mit Google Security Operations für Dashboard-, Berichterstellungs- und Speicherfunktionen. Der Kunde darf Looker und BigQuery im Rahmen von Google Security Operations nur gemäß den von Google vorgegebenen oder beschriebenen Bereitstellungs-, Konfigurations- und Nutzungseinschränkungen nutzen. Google kann dem Kunden im Zusammenhang mit seiner Nutzung von Looker Software bereitstellen, einschließlich Drittanbieter-Software. Bestimmte Software kann den Lizenzbedingungen von Drittanbietern unterliegen. Diese sind unter https://looker.com/trust-center/legal/notices-and-acknowledgements zu finden. Wenn der Kunde Google Security Operations oder Looker nicht mehr nutzt, wird er auch die Software nicht weiter verwenden. Google kann den Zugriff des Kunden auf Looker und/oder BigQuery jederzeit beenden, sollte dieser gegen die Vereinbarung verstoßen. Ungeachtet anderslautender Bestimmungen in dieser Vereinbarung bezeichnet der in diesem Unterabschnnitt 1(d)(ii) verwendete Begriff „Kundendaten“ (a) alle Daten in den Datenbanken des Kunden, die vom Kunden oder von den Endnutzern über Google Security Operations für Looker bereitgestellt werden, und (b) alle Ergebnisse, die dem Kunden oder den Endnutzern auf Abfragen solcher Daten über Looker bereitgestellt werden. Die Verpflichtungen von Google in Bezug auf Datenstandorte in Abschnitt 1 (Daten) der allgemeinen Dienstbedingungen gelten nicht für Dashboards, Berichte oder Speicher in Looker oder BigQuery.

iii. *Google SecOps Enterprise Plus*. Google (Chronicle) Security Operations Enterprise Plus beinhaltet Google Threat Intelligence. Wenn der Kunde, wie im Bestellformular ausgewiesen, die SKU SecOps Enterprise Plus abonniert, gelten neben diesen Nutzungsbedingungen für Google Security Operations auch die Nutzungsbedingungen für Google Threat Intelligence und VirusTotal in Unterabschnitt 3. Zur Klarstellung: Google Threat Intelligence ist nicht Teil der im Zusatz zur Verarbeitung von Cloud-Daten genannten geprüften Dienste und die Zusicherungen von Google in Bezug auf Datenstandorte in Abschnitt 1 (Daten) der allgemeinen Dienstbedingungen gelten nicht für Google Threat Intelligence.

iv. *Google Unified Security*. Wenn der Kunde, wie im Bestellformular ausgewiesen, die SKU Google Unified Security abonniert, gelten neben der Vereinbarung, einschließlich der Nutzungsbedingungen für Google Security Operations, die folgenden Zusatzbedingungen:

A. GCP-Dienstberechtigungen. Google Unified Security bietet Zugriff auf bestimmte Google Cloud Platform-Dienste. Dazu gehören Chrome Enterprise Premium, Security Command Center und Web Risk (wie in der Übersicht der Google Cloud Platform-Dienste beschrieben) (zusammenfassend die „GCP-Dienstberechtigungen"). Die Nutzung der GCP-Dienstberechtigungen durch den Kunden unterliegt der Vereinbarung, gemäß der Google dem Kunden die Google Cloud Platform bereitstellt, einschließlich der dienstspezifischen Nutzungsbedingungen für die Google Cloud Platform (und abgesehen von diesem Absatz gelten diese dienstspezifischen Nutzungsbedingungen für SecOps nicht für die GCP-Dienstberechtigungen). Zur Klarstellung: (i) die GCP-Dienstberechtigungen sind Google Cloud Platform-Dienste und nicht SecOps-Dienste, dies gilt auch für die Zwecke des Zusatzes zur Verarbeitung von Cloud-Daten, und (ii) die für GCP-Dienstberechtigungen geltenden SLAs sind unter https://cloud.google.com/terms/sla veröffentlicht; die Anwendung der gegebenenfalls in die Vereinbarung einbezogenen SLAs für SecOps-Dienste ist insoweit ausgeschlossen.

B. Zusätzliche SecOps-Berechtigungen. Google Unified Security umfasst außerdem Mandiant Threat Defense (eine Mandiant Managed Services-Berechtigung), Expertise On Demand und Google Threat Intelligence (zusammenfassend „Zusätzliche SecOps-Berechtigungen"). Die Nutzung der zusätzlichen SecOps-Berechtigungen durch den Kunden unterliegt den jeweiligen Nutzungsbedingungen der Dienste, wie sie in diesen SecOps-Nutzungsbedingungen aufgeführt sind. Zur Klarstellung: Google Threat Intelligence und Expertise On Demand gelten im Sinne des Zusatzes zur Verarbeitung von Cloud-Daten nicht als geprüfte Dienste und die Zusicherungen in Bezug auf Datenstandorte in Abschnitt 1 (Daten) der allgemeinen Dienstbedingungen gelten nicht für die zusätzlichen SecOps-Berechtigungen.

e. Servicegrenzen. Google kann die Eingabe von Daten durch einen Kunden in Google Security Operations beschränken, wenn diese die Kontingente („Quotas") überschreiten. Quotas werden durchgesetzt, um die Gemeinschaft der Nutzer von Google Security Operations zu schützen, indem unvorhergesehene Nutzungsspitzen und überlastete Dienste verhindert werden. Das Quota des Kunden ist im Konto angegeben. Weitere Informationen zu Quotas finden Sie in der Dokumentation.

f. *Fundierung mit der Google Suche*. Die „Fundierung mit der Google Suche" ist eine generative KI-Funktion von Google Security Operations, die fundierte Ergebnisse und Suchvorschläge bietet. „Fundierte Ergebnisse" sind Antworten, die Google anhand des Prompts des Kunden, anhand von Kontextinformationen, die der Kunde gegebenenfalls bereitstellt, und anhand von Ergebnissen der Suchmaschine von Google generiert. „Suchvorschläge" (engl.:"Search Suggestions" auch als „Einstiegspunkte für die Suche" oder engl. "Search Entry Points" bezeichnet) werden von Google zusammen mit den fundierten Ergebnissen zur Verfügung gestellt. Wenn auf ein fundiertes Ergebnis geklickt wird, gelten gesonderte Nutzungsbedingungen (nicht diese Nutzungsbedingungen) für die Landingpage. Wenn auf einen Suchvorschlag geklickt wird, unterliegt die Landingpage google.com den Google-Nutzungsbedingungen. Fundierte Ergebnisse und Suchvorschläge sind generierter Output. „Links" bezeichnet Möglichkeiten zum Aufrufen von Webseiten (einschließlich Hyperlinks und URLs), die möglicherweise in einem fundierten Ergebnis oder einem Suchvorschlag enthalten sind. Links umfassen auch Titel oder Labels, die zusammen mit diesen Möglichkeiten zum Aufrufen von Webseiten bereitgestellt werden. Der Kunde wird keine

Rechte an Gewerblichen Schutzrechten in Suchvorschlägen oder Links in fundierten Ergebnissen geltend machen, mit Ausnahme seiner kundeneigenen Webdomain.

i. *Nutzungseinschränkungen für die Fundierung mit der Google Suche*. Der Kunde:

A. wird die Fundierung mit der Google Suche nur im Zusammenhang mit der Nutzung von Google Security Operations und gemäß dieser Vereinbarung verwenden. Der Kunde zeigt die fundierten Ergebnisse mit den zugehörigen Suchvorschlägen nur dem Endnutzer an, der den Prompt gesendet hat.

B. wird fundierte Ergebnisse oder Suchvorschläge nicht speichern, im Cache speichern, kopieren, einbinden, strukturieren, syndizieren, weiterverkaufen, analysieren, für das Training oder sonstiges Lernen verwenden oder dafür Klick-Tracking, Link-Tracking oder andere Arten des Monitorings implementieren (außer wie unten beschrieben) und er wird dies auch Endnutzern oder Dritten nicht gestatten.

C. wird ohne schriftliche Genehmigung von Google (einschließlich in der Dokumentation):

1. die fundierten Ergebnisse oder Suchvorschläge nicht bearbeiten oder mit anderen Inhalten vermischen und

2. keine Zwischeninhalte (interstitial content) zwischen Links oder Suchvorschlägen und der zugehörigen Landingpage platzieren, Endnutzer von Landingpages wegleiten oder die vollständige Anzeige von Landingpages minimieren, entfernen oder anderweitig unterbinden.

ii. *Speicherung für Debugging und Tests*. Der Kunde nimmt zur Kenntnis, dass es für Google in angemessenem Umfang erforderlich ist, zum Zweck der Erstellung fundierter Ergebnisse und Suchvorschläge Prompts, Kontextinformationen, die der Kunde möglicherweise angibt, sowie generierte Ausgaben dreißig (30) Tage lang zu speichern. Da diese Informationen gespeichert werden, weist der Kunde Google an, dass die gespeicherten Informationen für Tests und das Debugging von Systemen genutzt werden können, die die Fundierung mit der Google Suche unterstützen.

iii. *Fortbestand*. Dieser Abschnitt (f) (Fundierung mit der Google Suche), sofern anwendbar, gilt auch nach Ablauf oder Beendigung dieser Vereinbarung weiterhin fort.

g. Weitere Definitionen.

„*Abgedeckte Mitarbeiter*“ bezeichnet Mitarbeiter oder Auftragnehmer des Kunden.

„*Kundennetzwerk*“ bezeichnet das vom Kunden für interne Geschäftszwecke genutzte Netzwerk sowie sämtliche Anwendungen, Software, Dienste und physischen Geräte, die für interne Geschäftszwecke genutzt werden und mit diesem Netzwerk verbunden sind.

„*Datenobergrenze*“ bezeichnet die Menge an Kundendaten, die der Kunde Google Security Operations ab dem Startdatum der Dienste pro Jahr über das Konto bereitstellen darf. Diese ist im Bestellformular als „Einheit(en)“ angegeben.

„*Mitteilungsfrist für Dateneinschränkungen*“ bedeutet entweder (a) 72 Stunden nach der Mitteilung von Google an den Kunden über die Nichteinhaltung oder (b) 7 Tage nach der Mitteilung von Google, falls der Kunde Google überzeugend darlegt, dass er angemessene Maßnahmen ergreift, um den Verstoß zu beseitigen..

„Datenzeitraum“ bezeichnet den im Bestellformular genannten Zeitraum, in dem Kundendaten in Google Security Operations verfügbar sind. Der Datenzeitraum wird auf Basis einer rollierenden, monatlichen Rückschau vom aktuellen Datum berechnet, das sich nach dem Zeitstempel des von Google Security Operations ausgelesenen Event-Datums bestimmt. Wenn im Bestellformular nichts anderes angegeben ist, beträgt der Datenzeitraum 12 Monate.

„Dokumentation“ bezeichnet die jeweils aktuelle Google Security Operations-Dokumentation, die Google seinen Kunden zur Nutzung der Dienste unter https://cloud.google.com/chronicle/docs zur Verfügung stellt.

„Generative KI-Funktion(en)“ wird im Sinne der Definition in den oben genannten allgemeinen Dienstbedingungen verwendet.

„Netzwerktelemetrie“ bezeichnet Sicherheitstelemetrie, die von Geräten generiert wird, die Teil des Kundennetzwerks sind, und umfasst keine Sicherheitstelemetrie, die von anderen Personen oder Stellen als den abgedeckten Mitarbeitern generiert wird. Beispielsweise umfasst die Netzwerktelemetrie keine Sicherheitstelemetrie, die von Kunden oder Partnern des Kunden generiert wird.

„Sicherheitstelemetrie“ bezeichnet Meta- oder andere Daten im Zusammenhang mit dem Sicherheitsstatus eines Kunden oder Endnutzers des Kunden, die von sicherheitsbezogenen Funktionen, Produkten oder Diensten erzeugt werden.

„Drittanbietertelemetrie“ bezeichnet Sicherheitstelemetriedaten, die der Kunde von einem Drittanbieter erhalten hat und die er zum Schutz des Kundennetzwerks nutzt.

„Einheiten“ bezeichnet die Einheiten, in denen die Nutzung eines Dienst-SKUs gemessen wird, beispielsweise Datenobergrenze oder abgedeckte Mitarbeiter.

2. Mandiant

a. Mandiant-Lösungen

i. Zugriff auf Mandiant-Lösungen. Vorbehaltlich der Vereinbarung, der Zahlung aller Gebühren und der etwaigen Geltung eines Scope of Use, kann der Kunde auf die in einem Bestellformular angegebenen Mandiant-Lösungen gemäß der Vereinbarung und allen Dokumentationen zugreifen und diese nutzen, dies aber ausschließlich für seine internen Geschäftszwecke.

1. Mandiant Security Validation. Mandiant Security Validation darf nur mit der über das Bestellformular gekauften Menge an Lizenzen genutzt werden. Kunden, die die „Validation on Demand“-Version von Mandiant Security Validation gekauft haben, erhalten eine Lizenz für 1 Akteur zur Durchführung 1 Bewertung, wie in der Dokumentation beschrieben, und diese Nutzung muss innerhalb von 1 Jahr ab dem Datum des jeweiligen Bestellformulars erfolgen. Die Laufzeit der Lizenz beginnt ab oder kurz nach dem Datum des Inkrafttretens des Bestellformulars (wie von Google festgelegt).

2. *Mandiant Attack Surface Management*. Kunden dürfen Mandiant Attack Surface Management nur im Rahmen der im Bestellformular erworbenen Lizenzrechte zum Zweck der Bewertung der Sicherheit von Assets nutzen, die über das Internet und im Zusammenhang mit ihrer Geschäftstätigkeit zugänglich sind.

3. *Intelligence-Abonnements*. Der Kunde kann verschiedene in der Dokumentation beschriebene Intelligence-Abonnements erwerben. Der Zugriff darauf wird über Zugriffsschlüssel oder Anmeldedaten gewährt, die von Endnutzern des Kunden nicht gemeinsam genutzt werden dürfen. Der Kunde darf keine Gruppenkonten anlegen. Google behält sich das Recht vor, die Anzahl und/oder Häufigkeit von Anfragen über die Intelligence-Abonnements zu beschränken, wie in der Dokumentation festgelegt. Zusätzlich zu allen anderen Rechten gemäß der Vereinbarung kann Google technische Maßnahmen ergreifen, um eine übermäßige Nutzung zu verhindern oder die Nutzung zu beenden, wenn Beschränkungen überschritten wurden.

4. *Mandiant Digital Threat Monitoring*. Der Kunde darf Mandiant Digital Threat Monitoring ausschließlich zur Analyse des eigenen Sicherheitsstatus verwenden. Google kann die Nutzung von Mandiant Digital Threat Monitoring durch den Kunden bei einem mutmaßlichen Verstoß gegen diesen Unterabschnitt 2(a)(i)(5) nach eigenem Ermessen beenden oder sperren.

ii. Sicherheitsinhalte.

1. *Lizenz*. Mandiant-Lösungen können Zugriff auf bestimmte definierte Dateien, URLs, IP-Adressen, Datei-Hashes, Befehle, Stichproben von Netzwerk-Traffic und andere Artefakte beinhalten, die schädlich sein und/oder reales Angriffsverhalten darstellen können („Sicherheitsinhalte“). Google gewährt dem Kunden eine eingeschränkte, nicht übertragbare, nicht exklusive Lizenz für die Nutzung der Sicherheitsinhalte ausschließlich im Zusammenhang mit den jeweiligen Mandiant-Lösungen und zu keinen anderen Zwecken. Von Dritten erhaltene oder lizenzierte Sicherheitsinhalte, die über Google bereitgestellt werden oder die der Kunde selbst beschafft, gelten als Angebot von Drittanbietern im Sinne der Vereinbarung. Google gewährleistet nicht, dass über Mandiant-Lösungen bereitgestellte Sicherheitsinhalte während der gesamten Laufzeit der Bestellung verfügbar sind, und Google kann Sicherheitsinhalte gelegentlich nach alleinigem Ermessen hinzufügen oder entfernen.

2. *Haftungsausschluss*. **Der Kunde ist sich bewusst, dass die Sicherheitsinhalte aktive Malware, einschließlich Ransomware, enthalten und dass die Verwendung der Sicherheitsinhalte in einer Weise, die von der in der Dokumentation ausdrücklich beschriebenen abweicht, Schäden an der Umgebung des Kunden verursachen kann. Die Sicherheitsinhalte werden „wie besehen“ bereitgestellt, und Google gibt keine Zusicherungen oder Gewährleistungen in Bezug auf die Sicherheitsinhalte und garantiert oder gewährleistet nicht, dass die Sicherheitsinhalte alle möglichen Bedingungen, Umgebungen oder Kontrollen abdecken. Die Sicherheitsinhalte stammen aus einer Vielzahl von Quellen, zu denen auch bekannte Bedrohungsakteure gehören können. Soweit dies nach geltendem Recht zulässig ist, übernimmt der Kunde alle mit der Nutzung der Sicherheitsinhalte verbundenen Risiken und erkennt an, dass Google nicht verpflichtet ist, sicherzustellen, dass die Sicherheitsinhalte bestimmungsgemäß funktionieren.**

3. *Übermittlung von Sicherheitsinhalten*. Mandiant-Lösungen gestatten dem Kunden möglicherweise, Sicherheitsinhalte oder andere Malware an Google zu übermitteln. Der Kunde nimmt zur Kenntnis, dass von ihm über die Mandiant-Lösungen bereitgestellte Sicherheitsinhalte oder andere Malware keine Kundendaten sind und von Google genutzt, aggregiert, analysiert und weitergegeben werden dürfen, um die Produkte und Dienste zu verbessern, die Google seinen Kunden zur Verfügung stellt.

b. Mandiant Managed Services

i. *Bereitstellung von Mandiant Managed Services*. Während der Laufzeit der Bestellung stellt Google Mandiant Managed Services gemäß den Angaben in der Dokumentation und entsprechend dem Umfang der vom Kunden erworbenen Berechtigungen oder Lizenzen bereit, die im jeweiligen Bestellformular angegeben sind. Alle vom Kunden angeforderten Mandiant Managed Services, die nicht in der Dokumentation beschrieben sind, werden zu einvernehmlich vereinbarten Preisen erbracht. Wenn die Anzahl der Berechtigungen oder Lizenzen das im Bestellformular angegebene gekaufte Volumen überschreitet, benachrichtigt Google den Kunden schriftlich und stellt eine Rechnung über die nächsthöhere Anzahl zu den dann geltenden Preisen von Google aus, anteilig für den verbleibenden Teil der dann geltenden Auftragsdauer. Die in diesen dienstspezifischen Bedingungen festgelegten Verpflichtungen von Google hinsichtlich des Speicherorts der Daten gelten nicht für Mandiant Managed Services.

ii. *Erwerb über Reseller und Partner*. Wenn der Kunde Mandiant Managed Services über einen von Google autorisierten Partner (ein „Partner“) erhält, erklärt sich der Kunde damit einverstanden, dass die Mandiant Managed Services und alle Ergebnisse der Mandiant Managed Services, einschließlich Berichten, über den Partner an den Kunden geliefert werden können. Ungeachtet anderslautender Bestimmungen in der Vereinbarung ermächtigt der Kunde Google, Informationen im Zusammenhang mit den Mandiant Managed Services und Kundendaten an den Partner weiterzugeben.

iii. *Pflichten des Kunden*. Der Kunde nimmt zur Kenntnis und erklärt sich damit einverstanden, dass (i) Mandiant Managed Services keine Alternative für Incident Response Engagement in einer Umgebung sind, die bereits vor der Laufzeit der Bestellung von Mandiant Managed Services kompromittiert ist, und (ii) die Fähigkeit von Google, die Mandiant Managed Services erfolgreich bereitzustellen, von der Fähigkeit des Kunden abhängt, seinen in diesem Unterabschnitt 2(b)(iii) aufgeführten Pflichten nachzukommen. Soweit gesetzlich zulässig, schließt Google die Haftung für die Nichtbereitstellung von Mandiant Managed Services aus, die darauf zurückzuführen ist, dass der Kunde sich weigert oder nicht in der Lage ist, seinen folgenden Pflichten nachzukommen:

1. *Installationsanforderungen*. Der Kunde ist für Folgendes verantwortlich: (i) Bereitstellung von Netzwerkarchitekturdiagrammen sowie physischem und logischem Zugriff auf die Umgebung des Kunden zu dem ausschließlichen Zweck, von Mandiant Managed Services unterstützte Technologie (wie gegebenenfalls in der Dokumentation definiert) zu installieren und zu konfigurieren, (ii) Upgrade bereits vorhandener Technologie auf die in der Dokumentation genannte Mindestsoftwareversion, (iii) Bestätigung, dass sämtliche Technologie in der Umgebung des Kunden erfolgreich gemäß dem Systemverwaltungsleitfaden und den unterstützten Konfigurationen des jeweiligen Produkts konfiguriert und mit dem Kundennetzwerk verbunden wurde, wie in den Supportbedingungen des entsprechenden Produkts festgelegt, und (iv) Bereitstellung der Möglichkeit der Einrichtung einer dauerhaften Verbindung zum Netzwerk des Kunden im festgelegten Portbereich, der dem Land entspricht, aus dem die Mandiant Managed Services bereitgestellt werden.

2. *Sicherheit von Anmeldedaten*. Der Kunde ist für Folgendes verantwortlich: (i) Bereitstellung korrekter Informationen, damit Google dem Personal des Kunden im Zusammenhang mit Mandiant Managed Services Zugriff auf Portale gewähren (und diesen wieder aufheben) kann, (ii) Umsetzung und Einhaltung hoher Standards für Passwörter, (iii) Bereitstellung korrekter

Informationen, damit Google Domains auf die Zulassungsliste setzen kann, und (iv) sofortige Meldung von Sicherheitsproblemen im Zusammenhang mit Mandiant Managed Services (einschließlich verfügbarer Portale) an Google.

3. *Ausschluss von Netzwerksegmenten*. Der Kunde informiert Google, falls bestimmte Netzwerksegmente kein Managed Defense-Monitoring erfordern. Wenn möglich, muss der Kunde detaillierte Informationen zum Netzwerksegmentbereich angeben (beispielsweise Gastnetzwerke, Testumgebungen).

4. *Behebung bekannter Kompromittierungen*. Der Kunde wird angemessene Anstrengungen unternehmen, um von Google oder Drittanbietern gemeldete bekannte Kompromittierungen zu beheben. Google kann von bekanntermaßen kompromittierten Systemen generierte Benachrichtigungen unterdrücken, bis die Kompromittierung behoben ist.

5. *Einstellung von Datum und Uhrzeit*. Der Kunde stellt sicher, dass die Einstellungen für Datum und Uhrzeit in sämtlicher unterstützter Technologie korrekt sind, damit mit einer Uhrzeit versehene Benachrichtigungen korrekt kategorisiert werden. Google ist nicht für die Meldung von Benachrichtigungen verantwortlich, die von unterstützter Technologie generiert werden, die keine aktuellen Einstellungen für Datum und Uhrzeit aufweisen.

iv. *Ausschlüsse*. Ungeachtet anderslautender Bestimmungen in der Vereinbarung ist Google nicht verpflichtet, die Mandiant Managed Services für (i) Produkte oder Dienstleistungen bereitzustellen, für die der Support eingestellt wurde oder die derzeit nicht unterstützt werden; (ii) Produkte oder Dienstleistungen, für die kein aktiver Support besteht; (iii) Produkte oder Dienstleistungen, auf die keine Updates angewendet wurden; (iv) Produkte oder Dienstleistungen, die nicht installiert und bereitgestellt wurden; oder (v) Produkte oder Dienstleistungen, die falsch konfiguriert oder falsch deployed wurden, wodurch die Überwachung durch die Mandiant Managed Services verhindert wird. Der Kunde nimmt zur Kenntnis, dass Google zur effizienten Erbringung der Mandiant Managed Services einige Features und Funktionen der zugrunde liegenden Produkte und Dienstleistungen kontrollieren kann, einschließlich durch die Anwendung von Updates, und dass diese Features oder Funktionen während der Laufzeit der Bestellung der Mandiant Managed Services möglicherweise nicht für die unabhängige Nutzung durch den Kunden verfügbar sind.

c. Mandiant Consulting Services

i. *Bereitstellung von Mandiant Consulting Services*. Google stellt dem Kunden die im Bestellformular angegebenen Mandiant Consulting Services, einschließlich Arbeitsergebnisse, bereit, sofern dieser seinen Pflichten gemäß des nachfolgenden Abschnitts 2(c)(v) (Verpflichtungen des Kunden) nachkommt. Arbeitsergebnisse gelten als abgeschlossen, wenn der Kunde ihre Abnahme schriftlich oder mündlich bestätigt, oder zehn (10) Arbeitstage, nachdem Google sie dem Kunden zur Verfügung gestellt hat, je nachdem, was zuerst eintritt. Mandiant Consulting Services umfassen keine Schulungsdienste.

ii. *Rechnungen und Zahlung*. Der Kunde zahlt alle Gebühren für Mandiant Consulting Services. Einige Gebühren sind gegebenenfalls, wie im Bestellformular angegeben, nicht stornierbar.

iii. *Eingesetzte Personen*. Google bestimmt, welche Personen die Mandiant Consulting Services erbringen. Wenn der Kunde einen Austausch der Personen fordert und eine geeignete und rechtmäßige Grundlage dafür nennt, unternimmt Google wirtschaftlich vernünftige Anstrengungen, um die zugewiesenen Personen durch andere Personen zu ersetzen. Wenn

Google vor Beginn der Mandiant-Beratungsdienste angemessene Personalschulungsrichtlinien des Kunden in Bezug auf die Mandiant-Beratungsdienste bereitgestellt werden, werden die Mitarbeiter von Google, die die Mandiant-Beratungsdienste erbringen, diese angemessenen Personalschulungsrichtlinien einhalten.

iv. *Einhaltung der geltenden Richtlinien und Verfahren am Kundenstandort*. Personen, die Google mit der Erbringung von Mandiant Consulting Services am Kundenstandort beauftragt, befolgen alle angemessenen vor Ort geltenden Richtlinien und Verfahrensanweisungen des Kunden, die Google vorab schriftlich mitgeteilt werden.

v. *Verpflichtungen des Kunden*.

1. *Kooperation*. Der Kunde wird Google bei der Erbringung der Mandiant-Beratungsdienste in angemessener Weise und zeitnah unterstützen. Google haftet nicht für Verzögerungen, die dadurch entstehen, dass der Kunde Google nicht die Informationen, Materialien, Zustimmungen oder den Zugang zu den Einrichtungen, Netzwerken, Systemen oder Schlüsselpersonen des Kunden zur Verfügung stellt, die Google zur Erbringung der Mandiant-Beratungsdienste benötigt. Wenn Google den Kunden über eine solche Unterlassung informiert und der Kunde die Unterlassung nicht innerhalb von 30 Tagen behebt, kann Google alle unvollständigen Mandiant-Beratungsdienste kündigen, und der Kunde hat die Google tatsächlich entstandenen Kosten für die stornierten Mandiant-Beratungsdienste zu tragen.

2. *Ausgaben*.

a. *Allgemein*. Der Kunde erstattet die Kosten, die im jeweiligen Bestellformular ausgewiesen sind.

b. *Rechtskosten*. Falls Google (einschließlich seiner verbundenen Unternehmen und seines Personals) vom Kunden dazu aufgefordert oder durch anwendbare Gesetze, ein gerichtliches Ersuchen oder behördliches Handeln dazu verpflichtet wird, im Hinblick auf die Mandiant Consulting Services oder die Vereinbarung Informationen, Dokumente oder Personal als Zeugen bereitzustellen, erstattet der Kunde Google (einschließlich seiner verbundenen Unternehmen und seines Personals, je nach Anwendungsfall) die Zeit, Aufwendungen und Verbindlichkeiten (einschließlich angemessener externer und interner Rechtskosten oder Bußgelder und Anwaltshonorare), die angefallen sind, um der Aufforderung nachzukommen, es sei denn, Google (einschließlich seiner verbundenen Unternehmen und seines Personals, je nach Anwendungsfall) ist selbst Verfahrensbeteiligter oder Gegenstand der Untersuchung.

3. *Versand von Medien*. Der Kunde nimmt zur Kenntnis und erklärt sich damit einverstanden, dass Google keine Verantwortung für Schäden trägt, die beim Versand und die Lieferung von Medien, Hardware und Geräten an Google entstehen.

4. *Informationen und Systeme*. Der Kunde ist allein für die Richtigkeit und Vollständigkeit aller Informationen verantwortlich, die er und sein Personal Google bereitstellen. Der Kunde sichert zu, dass er Eigentümer der zum Erbringen der Mandiant Consulting Services nötigen Systeme, Einrichtungen und/oder Geräte ist oder autorisiert ist, Google darauf Zugriff zu gewähren.

vi. Geistiges Eigentum.

1. *Background IP*. Der Kunde hält alle Rechte sowie das Eigentum und alle Ansprüche an dem bestehenden oder vorhandenen geistigen Eigentum des Kunden. Google hält alle Rechte sowie das Eigentum und alle Ansprüche an dem bestehenden oder vorhandenen geistigen Eigentum von Google. Zur Erbringung der Mandiant Consulting Services erteilt der Kunde Google eine Lizenz für die Nutzung des bestehenden oder vorhandenen geistigen Eigentums des Kunden (einschließlich eines Rechts zur Unterlizenzierung an verbundene Unternehmen oder Unterauftragnehmer von Google). Mit Ausnahme der Lizenzrechte aus den Unterabschnitten 2(c)(vi)(2) (Google-Technologie) und 2(c)(vi)(3) (Arbeitsergebnisse) unten erwirbt keine der Parteien durch diese Vereinbarung Rechte, Eigentum oder Ansprüche am bestehenden oder vorhandenen geistigen Eigentum der anderen Partei. Zur Klarstellung: Background IP ist von der Definition der „Freigestellte Materialien" (engl.: "Indemnified Materials") beider Parteien umfasst.

2. *Google-Technologie*. Google hält alle Rechte, Titel und Anteile an der Google-Technologie. Soweit die Google-Technologie in die Liefergegenstände integriert ist, gewährt Google dem Kunden eine beschränkte, weltweite, nicht ausschließliche, nicht übertragbare Lizenz (mit dem Recht zur Unterlizenzierung an verbundene Unternehmen) für die maximal nach geltendem Recht zulässige Dauer, um die Google-Technologie in Verbindung mit den Liefergegenständen für interne Geschäftszwecke des Kunden zu nutzen. Die Vereinbarung (einschließlich dieser servicespezifischen Bedingungen) gewährt dem Kunden kein Recht zur Nutzung von Materialien, Produkten oder Dienstleistungen, die Google-Kunden im Rahmen einer separaten Vereinbarung zur Verfügung gestellt werden.

3. *Liefergegenstände*. Google gewährt dem Kunden eine beschränkte, weltweite, nicht ausschließliche, vollständig bezahlte, nicht übertragbare Lizenz (mit dem Recht zur Unterlizenzierung an verbundene Unternehmen) für die maximal nach geltendem Recht zulässige Dauer zur Nutzung und Vervielfältigung der Liefergegenstände für interne Geschäftszwecke des Kunden.

vii. Gewährleistung und Rechtsbehelfe.

1. *Gewährleistung durch Google*. Google erbringt die Mandiant-Beratungsdienstleistungen auf professionelle und fachmännische Weise gemäß den Praktiken anderer Dienstleister, die ähnliche Dienstleistungen wie die Mandiant-Beratungsdienstleistungen erbringen. Google setzt für die Erbringung der Mandiant-Beratungsdienstleistungen Mitarbeiter mit den erforderlichen Fähigkeiten, Erfahrungen und Qualifikationen ein.

2. *Rechtsbehelfe*. Die Gewährleistungsrechte und die gesamte Haftung von Google für den Fall, dass Google Mandiant Consulting Services nicht gemäß Unterabschnitt 2(c)(vii)(1) (Gewährleistung durch Google) erbringt, sind darauf beschränkt, dass Google nach eigener Wahl (a) wirtschaftlich vernünftige Anstrengungen unternimmt, um die Mandiant Consulting Services noch einmal zu erbringen, oder (b) das Bestellformular kündigt und die jeweiligen Gebühren erstattet, die für die nicht vertragsgerecht erbrachten Mandiant Consulting Services angefallen sind. Ein Verstoß gegen die Gewährleistung gemäß Unterabschnitt 2(c)(vii)(1) (Gewährleistung durch Google) muss innerhalb von 30 Tagen nach dem Datum, an dem Google die jeweiligen Mandiant Consulting Services erbracht hat, geltend gemacht werden.

viii. Haftungsfreistellung.

1. *Ausschlüsse von der Haftungsfreistellung*. Die Abschnitte „Haftungsfreistellungsverpflichtungen von Google“ und „Haftungsfreistellungspflichten des Kunden“ der Vereinbarung gelten nicht, soweit der vom Dritten geltend gemachte Anspruch auf einem der folgenden Umstände beruht darauf beruht: (a) Änderungen an den freigestellten Materialien von Google oder den freigestellten Materialien des Kunden (je nach Anwendungsfall) durch eine andere als die freistellende Partei oder (b) Einhaltung von Anweisungen, Designvorgaben oder Anfragen für kundenspezifische Features oder Funktionen der freigestellten Partei.

2. *Gewährleistungsrechte bei Verletzungen*. Die im Abschnitt „Gewährleistungsrechte” der Vereinbarung beschriebenen Gewährleistungsrechte gelten auch für Liefergegenstände.

ix. Fortbestand. Die folgenden Unterabschnitte der Nutzungsbedingungen für Mandiant Consulting Services gelten nach Ablauf oder Beendigung der Vereinbarung oder des entsprechenden Bestellformulars weiterhin: 2(c)(vi) (Geistiges Eigentum), 2(c)(viii) (Haftungsfreistellung), 2(c)(ix) (Fortbestand) und 2(f) (Weitere Definitionen).

x. Versicherung. Während der Laufzeit der Vereinbarung unterhält jede Partei auf eigene Kosten einen angemessenen Versicherungsschutz, der für die Erfüllung der jeweiligen Verpflichtungen der Partei aus der Vereinbarung gilt, einschließlich einer Betriebshaftpflichtversicherung, Arbeitsunfallversicherung, Kfz-Haftpflichtversicherung und Berufshaftpflichtversicherung.

xi. Keine Werbung. Ungeachtet anderslautender Bestimmungen in der Vereinbarung, einschließlich der Abschnitte „Werbung” und „Anwendungsvorrang”, wird keine der Parteien ohne die vorherige schriftliche Zustimmung der anderen Partei öffentlich bekannt geben, dass Google Mandiant-Beratungsdienste für den Kunden erbringt.

xii. Google Cloud-Dienstdaten. Wenn der Kunde auch Cloud-Dienste (wie in der Google Cloud-Datenschutzerklärung definiert) erwirbt, gilt - ohne das damit Einschränkung der Verpflichtungen von Google gemäß der Google Cloud-Datenschutzerklärung in Bezug auf Dienstdaten verbunden sind - das Folgende:

1. Google kann auf diese Daten zugreifen und sie verarbeiten, um dem Kunden Mandiant-Beratungsdienste bereitzustellen, wie in der SecOps-Datenschutzerklärung näher beschrieben; und

2. Der Kunde wird die von dieser Verarbeitung betroffenen Personen gemäß den geltenden Gesetzen benachrichtigen.

d. Expertise On Demand.

i. *Bereitstellung von Expertise On Demand*. Google stellt dem Kunden die aktuellste Version der Dokumentation zur Verfügung, in der die über das Expertise On Demand-Abonnement („Expertise on Demand-Services“ oder „EOD“) verfügbaren Services beschrieben werden. Der Kunde kann während des zwölfmonatigen Zeitraums ab dem Datum des Inkrafttretens des Bestellformulars (der „abgedeckte Zeitraum“) alle in der Dokumentation beschriebenen Expertise on Demand-Services bestellen. Alle Expertise on Demand Services müssen innerhalb des Abdeckungszeitraums beginnen und innerhalb der in der Dokumentation festgelegten Fristen angefordert werden, damit die Terminplanung so erfolgen kann, dass die Expertise on Demand Services vor Ablauf des Abdeckungszeitraums beginnen können.

ii. *Einheiten*. Der Kunde zahlt eine feste Gebühr (die „Paket-Pauschalgebühr“), die ihn zu einer bestimmten Anzahl von Expertise-on-Demand-Einheiten („EOD-Einheiten“) berechtigt, wie in dem entsprechenden Bestellformular („Einheitenpaket“) angegeben. Die gesamte Paketpauschale wird am oder um das Datum des Inkrafttretens des Bestellformulars in Rechnung gestellt. Für jeden Expertise-on-Demand-Service wird die Anzahl der EOD-Einheiten abgezogen, die für diesen Expertise-on-Demand-Service in der Dokumentation aufgeführt sind. Der Kunde stellt jede Anfrage für Expertise-on-Demand-Services schriftlich gemäß der Beschreibung in der Dokumentation. Der Kunde kann während des Abdeckungszeitraums zusätzliche EOD-Einheiten („Zusatzeinheiten“) erwerben. Zusatz-Einheiten müssen während des Abdeckungszeitraums verwendet werden und sind nicht stornierbar und nicht erstattungsfähig. EOD-Einheiten (einschließlich Zusatz-Einheiten) dürfen nicht für Dienste verwendet werden, die nicht in der EOD-Dokumentation aufgeführt sind. Alle Technologiegebühren und -kosten werden gemäß der Dokumentation separat in Rechnung gestellt. EOD-Einheiten können zur Begleichung dieser Kosten verwendet werden.

iii. *Updates für Expertise On Demand-Dienste*. Der Kunde nimmt zur Kenntnis, dass Google die Dokumentation von Zeit zu Zeit aktualisieren kann und dass für die Expertise on Demand-Dienste stets die aktuellste Version der Dokumentation (einschließlich der Auflistungen der Expertise on Demand-Dienste und Einheitswerte) gilt. Ungeachtet des Vorstehenden wird Google den Kunden mindestens zwölf Monate im Voraus benachrichtigen, bevor ein Expertise on Demand-Dienst eingestellt oder die Anzahl der für einen Expertise on Demand-Dienst erforderlichen EOD-Einheiten erhöht wird.

iv. *Incident Response-Retainer*. Vorbehaltlich der Bedingungen für Mandiant Consulting Services bietet Google während des in der Dokumentation festgelegten Abdeckungszeitraums Incident-Response-Services („Incident-Response-Services“) an. Incident-Response-Services können Folgendes umfassen:

1. Support zur Reaktion auf Computersicherheitsvorfälle

2. Forensische, Log- und erweiterte Malware-Analyse

3. Erweiterten Support zur Reaktion auf Bedrohungsakteure

4. Erweiterte Unterstützung zur Behebung von Bedrohungen/Vorfällen

v. Zusatzbedingungen für Mandiant Services. Falls der Kunde im Rahmen seines Expertise On Demand-Abonnements Mandiant Consulting Services (einschließlich kundenspezifischer Intelligence-Briefings) oder Schulungsdienste bestellt, gelten Unterabschnitt 2(c) für Mandiant Consulting Services und Unterabschnitt 2(e) für Schulungsdienste.

e. Schulungsdienste

i. *Bereitstellung von Schulungsdiensten*. Vorbehaltlich etwaiger Schulungsbedingungen kann der Kunde Schulungsdienstleistungen für die Nutzung in Verbindung mit Mandiant-Produkten und -Dienstleistungen bestellen. Die Parteien vereinbaren einvernehmlich die Liefertermine und den Ort für die in einem Bestellformular angegebenen Schulungsdienstleistungen. Alle Schulungsdienstleistungen (einschließlich verschobener Schulungsdienstleistungen) müssen innerhalb eines Jahres ab dem Datum des Bestellformulars, mit dem die entsprechenden Schulungsdienstleistungen bestellt wurden, geplant und durchgeführt werden. Schulungsdienstleistungen umfassen keine Liefergegenstände.

1. *Private Schulungen.* Der Kunde muss die Verschiebung privater Schulungsdienstleistungen mindestens zwei Wochen vor dem geplanten Starttermin beantragen. Google wird sich in angemessener Weise bemühen, die Schulungsdienstleistungen je nach Verfügbarkeit zu verschieben, und der Kunde trägt alle mit der Verschiebung verbundenen Kosten, einschließlich der Änderung von Reiseplänen. Der Kunde darf keinen Teil der Schulungsdienstleistungen aufzeichnen.

2. *Öffentliche Schulungen.* Wenn der Kunde die Teilnahme an öffentlichen Schulungsleistungen storniert, muss er Google spätestens zwei (2) Wochen vor dem Datum der öffentlichen Schulungsleistungen darüber informieren, und Google wird dem Kunden eine Gutschrift in Höhe des für die öffentlichen Schulungsleistungen gezahlten Betrags ausstellen. Der Kunde muss Google über jede Ersetzung eines namentlich genannten Teilnehmers an öffentlichen Schulungsleistungen informieren. Google behält sich das Recht vor, Personen aus beliebigen Gründen die Teilnahme an öffentlichen Schulungsdienstleistungen zu verweigern. Wenn Google die Teilnahme verweigert, erstattet Google den für die öffentlichen Schulungsdienstleistungen dieser Person gezahlten Betrag. Google erstattet oder gutschreibt keine Gebühren für Teilnehmer, die nicht an den Schulungsdienstleistungen teilnehmen oder diese vorzeitig verlassen. Google behält sich das Recht vor, öffentliche Schulungsdienstleistungen aus beliebigen Gründen zu stornieren und eine Rückerstattung zu leisten. Der Kunde darf keinen Teil der Schulungsdienstleistungen aufzeichnen.

3. *On-Demand-Schulungen.* On-Demand-Schulungsdienste müssen innerhalb von 90 Tagen nach der Anmeldung absolviert werden. Der Kunde darf Anmeldedaten für On-Demand-Schulungsdienste nicht weitergeben oder übertragen.

f. Weitere Definitionen.

„Background IP" bezeichnet alle gewerblichen Schutzrechte, die eine Partei (a) vor dem Datum des Inkrafttretens des betreffenden Bestellformulars oder (b) unabhängig von den Diensten hält oder lizenziert.

„Liefergegenstände" bezeichnet schriftliche Berichte, die speziell für den Kunden als Ergebnis der gemäß der Vereinbarung erbrachten Mandiant Consulting Services erstellt werden.

„Dokumentation" bezeichnet die jeweils aktuelle Mandiant-Dokumentation, die Google seinen Kunden auf Anfrage zur Nutzung der Dienste zur Verfügung stellt.

„Google Cloud-Datenschutzhinweise" bezeichnet die jeweils aktuellen Google Cloud-Datenschutzhinweise unter https://cloud.google.com/terms/cloud-privacy-notice.

„Google-Technologie" bezeichnet (a) bestehendes oder vorhandenes geistiges Eigentum von Google, (b) jedwedes geistiges Eigentum und Fachwissen mit Bezug zu Google-Produkten und -Diensten, (c) Kompromittierungsindikatoren und (d) Tools, Code, Algorithmen, Module, Materialien, Dokumentation, Berichte und Technologie, die in Verbindung mit den Diensten entwickelt werden und allgemeine Anwendung bei anderen Google-Kunden finden, einschließlich Arbeiten, die von bestehendem oder vorhandenem geistigem Eigentum von Google abgeleitet wurden oder dieses verbessern. Google-Technologie schließt weder Background IP des Kunden noch vertrauliche Informationen des Kunden ein.

„Kompromittierungsindikatoren“ oder *„Indikatoren“* bezeichnet Spezifikationen von Anomalien, Konfigurationen oder anderen Bedingungen, die Google innerhalb einer IT-Infrastruktur identifizieren kann und die von Google bei der Erbringung der Dienste verwendet werden.

„Bestellformular“ bezeichnet ein Bestellformular, eine Leistungsbeschreibung oder ein anderes Dokument, das von Google im Rahmen der Vereinbarung ausgestellt wird, einschließlich Datenblätter zu den im Bestellformular beschriebenen Diensten, und das vom Kunden und von Google unterzeichnet wird und in dem die Dienste festgelegt sind, die Google für den Kunden erbringen wird.

„Eingesetzte Personen“ bezeichnet die jeweiligen Geschäftsführer, Führungskräfte, Mitarbeiter, Vertreter und Subunternehmer einer Partei und ihrer verbundenen Unternehmen.

„SecOps-Datenschutzhinweise“ bezeichnet die jeweils aktuellen SecOps-Datenschutzhinweise unter https://cloud.google.com/terms/secops/privacy-notice.

„Dienstdaten“ hat die in den Google Cloud-Datenschutzhinweisen festgelegte Bedeutung.

„Bedingungen für Schulungen“ bezeichnet die jeweils aktuellen Bedingungen für Schulungsdienste, die Google für den Kunden erbringt.

3. Google Threat Intelligence und VirusTotal („GTI“)

a. Zugriff und Nutzung. Vorbehaltlich der Vereinbarung, der Zahlung aller Gebühren und der etwaigen Geltung eines Scope of Use, kann der Kunde auf GIT zugreifen und GIT nutzen, wie im Bestellformular und dem Platform Security Content angegeben, dies jedoch ausschließlich für seine interne Geschäftszwecke. Der Zugriff des Kunden auf sein GTI-Konto wird ermöglicht über Zugriffsschlüssel, einschließlich Google-APIs, oder Anmeldedaten, die der Kunde jeweils nicht an Dritte weitergeben darf. Google behält sich das Recht vor, die Anzahl und/oder Häufigkeit der Anfragen des Kunden über GTI gemäß den Angaben in der Dokumentation zu begrenzen. Zusätzlich zu allen anderen Rechten aus der Vereinbarung kann Google technische Maßnahmen ergreifen, um eine übermäßige Nutzung zu verhindern oder die Nutzung nach Überschreiten der Beschränkungen zu unterbinden.

b. Einschränkungen. Sofern in diesen GTI-Servicebedingungen nicht ausdrücklich anders angegeben, ist es dem Kunden untersagt, Folgendes zu tun oder Endnutzern, einschließlich Endnutzern von Kundenprodukten, zu gestatten:

i. Platform Security Content oder GTI-Ergebnisse, einschließlich, aber nicht beschränkt auf Google-APIs oder Schnittstellen oder Teile davon direkt oder indirekt an Dritte unterlizenzieren, vertreiben, öffentlich vorführen oder wiedergeben oder anderweitig teilen oder zugänglich machen.

ii. Platform Security Content zu beschaffen oder zu nutzen, sofern dies nicht ausdrücklich gestattet ist, oder GTI zu nutzen oder zu versuchen, GTI zu nutzen, um Informationen in einer Weise zu gewinnen, die Rückschlüsse auf die Identität einzelner privater Personen zulässt, oder zu versuchen, auf Inhalte von Platform Security Content zuzugreifen oder diese zu missbrauchen, oder GTI oder Platform Security Content anderweitig für andere Zwecke als zur Erkennung und Abwehr von Malware in nichtkommerzieller persönlicher oder organisatorischer Eigenschaft zu verwenden.

iii. Der Platform Security Content, die der Kunde über GTI erhält, ohne die ausdrückliche schriftliche Genehmigung des jeweiligen Sicherheitspartners öffentlich einem Sicherheitspartner (einschließlich, aber nicht beschränkt auf Antiviren-Anbieter, URL-Scan-Engines, Dateicharakterisierungstools usw.) zuordnen.

Die in diesem Absatz (b) aufgeführten Einschränkungen gelten als „Einschränkungen“ oder „Nutzungseinschränkungen“ im Sinne der Vereinbarung.

c. Dienstsperrung. Google kann den Zugriff des Kunden auf GTI sperren, wenn dieser sich nicht an Unterabschnitte 3(a) (Zugriff und Nutzung) oder Paragraf 3(h)(ii)(C) dieser Nutzungsbedingungen für GTI hält, sofern Google den Kunden unverzüglich über die Sperrung informiert, soweit dies rechtlich zulässig ist.

d. **Haftungsausschluss. Der Kunde ist sich bewusst, dass der Platform Security Content Live-Malware, einschließlich Ransomware, umfasst und dass die Verwendung des Platform Security Content in einer Weise, die von der in der Dokumentation ausdrücklich beschriebenen abweicht, Schäden an der Umgebung des Kunden verursachen kann. Platform Security Content wird “wie besehen“ bereitgestellt, und Google gibt keine Zusicherungen oder Gewährleistungen in Bezug auf den Platform Security Content und garantiert oder gewährleistet nicht, dass der Platform Security Content alle möglichen Bedingungen, Umgebungen oder Kontrollen abdeckt. Der Platform Security Content stammt aus einer Vielzahl von Quellen, zu denen auch bekannte Bedrohungsakteure gehören können. Soweit dies nach geltendem Recht zulässig ist, übernimmt der Kunde alle mit der Nutzung des Platform Security Contents verbundenen Risiken und erkennt an, dass Google nicht verpflichtet ist, sicherzustellen, dass der Platform Security Content bestimmungsgemäß funktioniert.**

e. Vom Kunden übermittelte Inhalte und Inhaltsrichtlinien der Community.

i. Der Kunde kann Google vom Kunden übermittelte Inhalte bereitstellen. Der Kunde nimmt zur Kenntnis und erklärt sich damit einverstanden, dass Google vom Kunden übermittelte Inhalte nutzen, aggregieren, analysieren und diese unter anderem an Sicherheitspartner weitergeben kann, um die Produkte und Dienste von Google und seinen Sicherheitspartnern zu verbessern. Der Kunde erklärt, dass (i) vom Kunden übermittelte Inhalte der Vereinbarung und den SecOps-Datenschutzhinweisen entsprechen und (ii) er entweder der ursprüngliche Eigentümer der vom Kunden übermittelten Inhalte ist oder alle notwendigen Rechte und Berechtigungen hat, um die vom Kunden übermittelten Inhalte sowie verwandte Informationen unwiderruflich beizutragen und zu teilen, unter anderem mit der Community.

ii. Der Kunde bleibt Eigentümer seines Originalmaterials in den vom Kunden übermittelten Inhalten. Soweit gesetzlich zulässig, gewährt der Kunde Google (und denjenigen, mit denen Google arbeitet) durch das Hochladen oder Senden von vom Kunden übermittelten Inhalten eine weltweit gültige, gebührenfreie, unbefristete, unwiderrufliche und übertragbare Lizenz, um sämtliche Inhalte in vom Kunden übermittelten Inhalten zu verwenden, zu bearbeiten, zu hosten, zu speichern, zu reproduzieren, zu ändern, abgeleitete Werke daraus zu erstellen, zu kommunizieren, zu veröffentlichen, öffentlich vorzuführen, öffentlich wiederzugeben und zu vertreiben.

iii. DER KUNDE ERKLÄRT SICH DAMIT EINVERSTANDEN, DASS ER NUR VOM KUNDEN ÜBERMITTELTE INHALTE HOCHLADEN WIRD, DIE ER ÖFFENTLICH TEILEN MÖCHTE, UND DASS ER NICHT OHNE RECHTMÄßIGE ERLAUBNIS WISSENTLICH VOM KUNDEN ÜBERMITTELTE

INHALTE AN GTI SENDEN WIRD, DIE VERTRAULICHE ODER WIRTSCHAFTLICH SENSIBLE DATEN BEINHALTEN. AUßERDEM STIMMT DER KUNDE ZU, DASS ER KEINE VOM KUNDEN ÜBERMITTELTEN INHALTE AN GTI SENDEN WIRD, DIE PERSONENBEZOGENE DATEN BEINHALTEN.

iv. Obwohl Google nicht verpflichtet ist, die Nutzung von GTI, Nutzerinhalte oder vom Kunden eingereichte Inhalte zu überwachen, kann Google GTI überwachen, um betrügerische Aktivitäten oder Verstöße gegen die Vereinbarung aufzudecken und zu verhindern, und behält sich das uneingeschränkte Recht vor, vom Kunden übermittelte Inhalte, Materialien oder Nutzer jederzeit und ohne Angabe von Gründen ohne vorherige Ankündigung aus GTI zu entfernen. Um die Sicherheit der Community und die Verantwortlichkeit für den Informationsaustausch zu fördern, werden Konten und von Kunden übermittelte Inhalte, die von der Community beigesteuert wurden (z. B. Kommentare, Beiträge usw.), in der Regel nicht aus GTI entfernt, es sei denn, sie sind illegal, verletzen die gesetzlichen Rechte einer Person, dienen anderen unethischen/böswilligen Zwecken oder verstoßen anderweitig gegen die Vereinbarung.

v. WENN DER KUNDE VOM KUNDEN ÜBERMITTELTE INHALTE NICHT ÖFFENTLICH TEILEN MÖCHTE, WIE IN DER VEREINBARUNG ODER DEN SECOPS-DATENSCHUTZHINWEISEN FESTGELEGT, SENDET DER KUNDE DIESE NICHT AN GTI, DA SINN UND ZWECK DES DIENSTES DIE AGGREGATION UND WEITERGABE VON BEDROHUNGSINFORMATIONEN AN UND ÜBER DIE COMMUNITY IST.

vi. Private Scanning. Wenn der Kunde, wie im Bestellformular konkretisiert, die SKU Private Scanning abonniert, werden ungeachtet dieses Unterabschnitts 3(e) vom Kunden übermittelte Inhalte, die vom Kunden über die GTI-Funktion Private Scanning („Private Scanning“) hochgeladen werden, nicht mit anderen Kunden, Sicherheitspartnern oder der Community geteilt, außer sie werden zusätzlich in den GTI-Standarddienst hochgeladen.

f. Einstellung und Kündigung.

i. Ungeachtet anderslautender Bestimmungen in der Vereinbarung kann Google neue Dienste, Features oder Funktionen ohne vorherige schriftliche Ankündigung gegenüber dem Kunden einstellen. Neue Dienste, Features oder Funktionen unterliegen möglicherweise Zusatzbedingungen, die dem Kunden mitgeteilt werden.

ii. Bei Kündigung oder Ablauf dieser Vereinbarung oder des jeweiligen Bestellformulars löscht der Kunde sofort sämtlichen Platform Security Content, einschließlich solchem aus Cloud-Repositories, Dateiverzeichnissen, Datenträgern oder anderen Orten oder Instanzen, an denen sie gespeichert sein können, und nutzt und erstellt keine Produkte oder Dienste mehr, die verbleibenden Platform Security Content beinhalten.

g. Browsererweiterung. Wenn der Kunde über die Browsererweiterung auf GTI zugreift, erfasst Google Informationen darüber, wie die Domainnamen, die der Kunde besucht, aufgelöst werden. Daten passiver Domain Name Systems („pDNS“) umfassen Domainnamen, die über den Browser des Kunden angefordert werden, sowie die Auflösung der IP-Adressen dieser Domainnamen. Google stellt diese pDNS-Daten über GTI zur Verfügung, damit Mitglieder der Community schädliche Domains besser erkennen können, die möglicherweise auf einem von einem Angreifer kontrollierten Server, der über eine bestimmte IP-Adresse kontaktiert wird, gehostet werden. Die erfassten pDNS-Daten unterscheiden sich vom Browserverlauf und sind nie mit einem Nutzer verknüpft beziehungsweise werden nicht verwendet, um eine Person zu identifizieren. Nutzer, die die Browsererweiterung bereits verwenden, müssen der Weitergabe von pDNS-Daten an die

Community erst zustimmen. Nutzer, die die Browsererweiterung zum ersten Mal herunterladen, können die Datenerfassung in den Einstellungen der Browsererweiterung deaktivieren.

h. SKUs für die GTI-Einbindung. Zusätzlich zu diesen Nutzungsbedingungen für GTI gelten die folgenden Zusatzbedingungen im Hinblick auf SKUs für die GTI-Einbindung.

i. *Zulässige Nutzung*. Während der Laufzeit und ungeachtet der Anforderungen für interne Geschäftszwecke in Abschnitt 3(a) dieser GTI-Servicebedingungen darf der Kunde Platform Security Content zur Verbesserung der Kundenprodukte nutzen, vorausgesetzt, dass (a) die Kundenprodukte einen von GTI unabhängigen materiellen Wert haben und (b) der Kunde die Vereinbarung einhält.

ii. *Einschränkungen*. Der Kunde wird nicht:

A. Dritten, einschließlich Endnutzern von Kundenprodukten, Zugriff auf das GTI-Konto des Kunden, auf Google-APIs oder auf Platform Security Content gewähren, außer für GTI-Widget-Daten wie in Unterabschnitt 3(h)(iv)(A) dieser Nutzungsbedingungen für GTI ausdrücklich gestattet,

B. GTI oder Platform Security Content in oder zum Trainieren von auf künstlicher Intelligenz basierenden Modellen verwenden,

C. GTI oder Platform Security Content nutzen, um Kundenprodukte oder andere Produkte oder Dienste zu entwickeln, anzubieten, zu unterstützen oder zu verbessern, die in Konkurrenz zu Google Security Operations oder GTI stehen, oder

D. im Hinblick auf GTI oder Platform Security Content irgendwelche Zusicherungen oder Gewährleistungen geben.

Die in diesem Absatz (h)(ii) aufgeführten Einschränkungen gelten als „Einschränkungen“ oder „Nutzungseinschränkungen“ im Sinne der Vereinbarung.

iii. *Anforderungen*. Der Kunde wird:

A. sich an die Dokumentation zu GTI-Einbindungen halten,

B. allein für den technischen Support seiner Kundenprodukte verantwortlich sein und

C. sicherstellen, dass jeglicher Verkauf von Kundenprodukten einer durchsetzbaren Endnutzervereinbarung unterliegt, die bis zum Ende der jeweiligen Laufzeit der Bestellung gültig bleibt, außer die Vereinbarung wird vorher beendet. Unbeschadet der Verpflichtungen, die Google gegenüber dem Kunden im Rahmen dieser Vereinbarung eingegangen ist, übernimmt Google, soweit gesetzlich zulässig, keine Verantwortung oder Haftung gegenüber dem Kunden oder den Endnutzern von Kundenprodukten im Hinblick auf (a) jegliche Endnutzervereinbarung oder (b) den Zugriff auf sowie Bereitstellung oder Nutzung von GTI, dem GTI-Widget oder Platform Security Content durch den Kunden für oder im Namen der Endnutzer von Kundenprodukten.

iv. GTI-INT-Advanced und GTI-INT-Custom SKUs. Wenn nicht anders angegeben, gelten die folgenden Zusatzbedingungen für die SKUs GTI-INT-Advanced und GTI-INT-Custom.

A. *GTI-Widget*. Ungeachtet des Unterabschnitts 3(b)(i) dieser Nutzungsbedingungen für GTI darf der Kunde mithilfe von Google-APIs das GTI-Widget in Kundenprodukte ausschließlich zu

dem Zweck einbinden, um die Sicherheitstelemetriedaten von Endnutzern des Kunden durch GTI-Widget-Daten zu ergänzen. Der Kunde darf GTI-Widget-Daten Endnutzern von Kundenprodukten nur visuell wiedergeben. Der Kunde ist für den Zugriff von Endnutzern von Kundenprodukten auf das GTI-Widget und deren Nutzung von GTI-Widget-Daten verantwortlich. Wenn der Kunde Endnutzern von Kundenprodukten GTI-Widget-Daten anzeigt, wird er den klar und deutlich erkennbaren Hinweis „Angereichert durch Google Threat Intelligence“ aufnehmen.

B. *Öffentliche Materialien*.

1. Der Kunde darf Unterlagen und Begleitmaterial zu Kundenprodukten, einschließlich Blogs, Whitepapers und Verkaufsmaterialien („Öffentliche Materialien“) veröffentlichen. Alle öffentlichen Materialien müssen den klar und deutlich erkennbaren Hinweis „Angereichert durch Google Threat Intelligence“ gemäß den Branding-Leitlinien tragen, die Google dem Kunden zur Verfügung stellt. Der Kunde ist allein dafür verantwortlich, sicherzustellen, dass alle öffentlichen Materialien geltendem Recht, einschließlich der Datenschutzgesetze, entspricht.

2. Ungeachtet des Unterabschnitts 3(h)(iv)(B)(1) darf der Kunde keine anderen Informationen über Google oder seine Produkte oder Dienste, einschließlich GTI, veröffentlichen oder Markenkennzeichen von Google ohne vorherige schriftliche Genehmigung durch Google verwenden. Dies gilt für die Veröffentlichung in öffentlichen Materialien oder in einem anderen Medium.

C. GTI-INT-Custom. Sofern nichts anderes in einem Bestellformular vereinbart wurde, gelten die folgenden Zusatzbedingungen nur für die SKU GTI-INT-Custom:

1. *Berichte*.

   a. Erforderliche Informationen. Der Kunde stellt Google für jeden Berichtszeitraum einen Bericht (jeweils ein „Bericht“) zur Verfügung. Jeder Bericht enthält mindestens die folgenden Informationen ausschließlich zum Zweck der Rechnungsstellung durch Google und der Überprüfung, ob der Kunde die Vereinbarung einhält:

   - Anzahl der aktiven Endnutzer von Kundenprodukten sowie Anzahl der vom Kunden verwalteten Assets
   - Einnahmen des Kunden aus den Kundenprodukten
   - Anzahl der Mitarbeiter, Branche und Standort der Endnutzer von Kundenprodukten (jeweils soweit gesetzlich zulässig)

   b. *Einreichung*. Jeder Bericht muss jeweils innerhalb von 30 Tagen nach Ablauf des entsprechenden Berichtszeitraums eingereicht werden. Er deckt den Zeitraum ab dem Tag nach Ende des vorherigen Berichtszeitraums bis zum Ende des aktuellen Berichtszeitraums ab.

   c. *Abnahme*. Innerhalb von zehn (10) Werktagen nach Erhalt eines Berichts kann Google in gutem Glauben die Richtigkeit eines Berichts bestreiten. Im Falle eines solchen Bestreitens werden der Kunde und Google in gutem Glauben daran arbeiten, die Streitigkeit beizulegen, wozu auch gehört, dass der Kunde unverzüglich auf alle

zumutbaren Anfragen von Google reagiert und Google auf Anfrage die zur Beilegung der Streitigkeit erforderlichen Unterlagen zur Verfügung stellt. Nach der Abnahme durch Google gilt der Bericht für den betreffenden Berichtszeitraum als akzeptiert, und Google verzichtet auf jegliches weitere Recht, die Richtigkeit des Berichts anzufechten.

d. *Erweiterung*. Wenn der Kunde mehr Einheiten verbraucht als während der Laufzeit der Bestellung gekauft (ersichtlich aus dem Bericht/den Berichten), informiert Google den Kunden darüber, und die Parteien unterzeichnen ein Bestellformular über die zusätzlichen Einheiten.

v. Zusätzliche Haftungsfreistellungspflichten des Kunden. Zusätzlich zu den in der Vereinbarung festgelegten Haftungsfreistellungspflichten des Kunden wehrt der Kunde Ansprüche Dritter gegen Google und die mit Google verbundenen Unternehmen ab und stellt diese von Ansprüchen Dritter in Gerichtsverfahren frei, soweit sich diese Ansprüche ergeben aus (a) den Kundenprodukten, (b) vom Kunden übermittelten Inhalten und (c) dem Zugriff auf und der Nutzung von Platform Security Content durch den Kunden und die Endnutzer von Kundenprodukten.

i. *Nutzer, die VirusTotal kostenlos verwenden.* Die SLAs, die Freistellungsverpflichtungen von Google gemäß der Vereinbarung sowie die Richtlinien für technische Supportdienste gelten nicht für Nutzer, die VirusTotal kostenlos verwenden. Ausschließlich für Nutzer, die VirusTotal kostenlos verwenden, wird die Definition von „Dienste“ in der Vereinbarung durch Folgendes ersetzt:

„Dienste“ bezeichnet den VirusTotal-Dienst und die Plattform zur Erkennung von Malware, die reale Bedrohungsinformationen nutzen, die von einer weltweiten Community von Nutzern stammen.

j. *VirusTotal-Bestandskunden.* Auf den Erwerb und die Nutzung von VirusTotal finden anstatt der Vereinbarung die Nutzungsbedingungen für VirusTotal Enterprise unter https://go.chronicle.security/hubfs/vt_terms.pdf oder eine Offlineversion davon, sofern verfügbar, Anwwendung, sofern der Kunde VirusTotal von Chronicle LLC oder Chronicle Security Ireland Limited erworben hat.

k. Weitere Definitionen.

„*Assets*“ bezeichnet physische oder virtuelle Hardware- oder Softwaresicherheitsgeräte, die durch Kundenprodukte geschützt werden.

„*Browsererweiterung*“ ist die unter https://docs.virustotal.com/docs/browser-extensions beschriebene Browsererweiterung.

„*Community*“ bezeichnet ein Mitglied der Öffentlichkeit, AV-, Scan-, Sandbox- oder andere Sicherheitspartner, sicherheitsbewusste Organisationen und andere lizenzierte Nutzer des Dienstes.

„*Endnutzer von Kundenprodukten*“ bezeichnet eine dritte Person oder Entität, die mit dem Kundenprodukt beziehungsweise den Kundenprodukten interagiert. Endnutzer von Kundenprodukten dürfen das Kundenprodukt beziehungsweise die Kundenprodukte nur

verwenden, um ihre eigenen internen Mitarbeiter, Daten, Systeme, Netzwerke, Anwendungen, Nutzer und Prozesse zu schützen.

„Kundenprodukt(e)“ „ bezeichnet ein Angebot, das der Kunde mithilfe von GTI oder gemäß den Angaben in einem Bestellformular verbessert oder herstellt. Kundenprodukte umfassen nicht GTI.

„Vom Kunden übermittelte Inhalte“ bezeichnet sicherheitsrelevante Objekte und Artefakte, einschließlich ausführbarer und nicht ausführbarer Dateien, die in GTI hochgeladen oder von GTI gescannt oder analysiert werden, einschließlich durch Tools auf der Website durch GTI-Nutzer, sowie zugehörige Metadaten, Kommentare und/oder Beiträge, die über GTI zur Verfügung gestellt werden. Zur Klarstellung: Vom Kunden übermittelte Inhalte sind keine Kundendaten.

„Dokumentation“ bezeichnet die jeweils aktuelle Dokumentation, die Google seinen Kunden für die Nutzung von GTI zur Verfügung stellt, wie unter https://docs.virustotal.com und https://gtidocs.virustotal.com/ beschrieben und wie sonst auf Anfrage des Kunden durch Google bereitgestellt.

„Endnutzervereinbarung“ bezeichnet eine Vereinbarung zwischen dem Kunden und einem Endnutzer von Kundenprodukten, gemäß der der Kunde Kundenprodukte verkauft oder liefert.

„Dokumentation zu GTI-Einbindungen“ bezeichnet die jeweils aktuelle Dokumentation, die Google Kunden für die Nutzung der SKUs für die GTI-Einbindung unter http://www.virustotal.com/go/gti-integration-skus-docs zur Verfügung stellt.

„SKUs für die GTI-Einbindung“ bezeichnet die GTI-SKUs, die (i) zum Datum des Inkrafttretens des Bestellformulars unter https://assets.virustotal.com/google-ti-integration-packages.pdf aufgeführt sind und (ii) über (A) ein unterzeichnetes Bestellformular direkt bei Google oder (B) im Rahmen einer Reseller-Vereinbarung bei einem Reseller bestellt werden. Zur Klarstellung sei erwähnt, dass die SKUs für die GTI-Einbindung GTI-INT-Core, GTI-INT-Advanced und GTI-INT-Custom umfassen.

„GTI-Widget“ bezeichnet ein HTML-Widget, das der Kunde über eine Google-API in Kundenprodukte einbindet und das es dem Kunden ermöglicht, Endnutzern von Kundenprodukten GTI-Widget-Daten anzuzeigen.

„GTI-Widget-Daten“ hat die in der Dokumentation zur GTI-Einbindung beschriebene Bedeutung und bezeichnet auch jegliche Zusammenfassungen, abgeleitete Berichte und Metadaten, die der Kunde über GTI aus GTI-Widget-Daten ableitet.

„Interne Geschäftszwecke“ bedeutet den Schutz der internen Mitarbeiter, Daten, Systeme, Netzwerke, Anwendungen, Nutzer und Prozesse des Kunden.

“Platform Security Content” bezeichnet alle Inhalte oder Daten, mit denen der Kunde über GTI interagieren oder die er von GTI abrufen kann, einschließlich Dateien, URLs, IP-Adressen, Domains, Datei-Hashes, Befehlen, Stichproben des Netzwerk-Traffics, vom Kunden übermittelten Inhalten, GTI-Widget-Daten, Google-Berichten, ausgewählten Sammlungen (einschließlich, aber nicht beschränkt auf Akteure, Kampagnen, Malware, Sicherheitslücken), Google-Attributionen/-Verknüpfungen zu Sicherheitslückenobjekten, Benachrichtigungen, Deep-/Dark-Web-Daten, Analystenkommentaren und -annotationen, YARA-Signaturen und Inhalten/Analysen in Bezug auf Taktiken, Techniken und Prozeduren (TTP) oder Bedrohungsprofilen und anderen Artefakten, die schädlich sein und/oder reales Angriffsverhalten darstellen können.

„*Berichtszeitraum*“ bezeichnet das Zeitintervall, das ein Bericht abdeckt, sowie die Häufigkeit, in der Berichte vorgelegt werden müssen. Ein jährlicher Berichtszeitraum bedeutet beispielsweise, dass ein Bericht ein Jahr abdeckt und jährlich ein Bericht eingereicht werden muss. Für den ersten Bericht beginnt der Berichtszeitraum ab dem Datum des Inkrafttretens des Bestellformulars. Google setzt den Kunden schriftlich über den Berichtszeitraum in Kenntnis, sofern im Bestellformular nichts anderes festgelegt ist. Wenn von Google oder im Bestellformular nichts anderes schriftlich festgelegt ist, gilt ein jährlicher Berichtszeitraum.

„*Scope of Use*“ wird im Sinne der Definition in den oben genannten allgemeinen Dienstbedingungen verwendet.

„*SecOps-Datenschutzhinweise*“ bezeichnet die jeweils aktuellen SecOps-Datenschutzhinweise unter https://cloud.google.com/terms/secops/privacy-notice.

„*Sicherheitspartner*“ bezeichnet Mitglieder der Öffentlichkeit, Antivirus-, Scan-, Sandbox- oder andere Sicherheitspartner, die vom Kunden übermittelte Inhalte nutzen und in GTI beitragen.

„*Sicherheitstelemetrie*“ wird im Sinne der Definition in den obigen Nutzungsbedingungen für Google Security Operations verwendet. Sicherheitstelemetrie umfasst nur Metadaten oder andere Daten, die unabhängig in die Kundenprodukte aufgenommen werden und nicht über GTI.

„*Website*“ bezeichnet die Website unter virustotal.com sowie alle durch Google und seine verbundenen Unternehmen mit virustotal.com verknüpften gesteuerten und zur Marke VirusTotal gehörenden Websites.

„*Einheiten*“ bezeichnet die Einheiten, in denen die Nutzung einer SKU für die GTI-Einbindung gemessen wird, beispielsweise Anzahl der Kundenprodukte.

4. Security Customer Success Services.

a. *Anwendbare Nutzungsbedingungen*. Die Bedingungen in den Unterabschnitten 2(c) (Mandiant Consulting Services) und 2(f) (Weitere Definitionen) dieser Nutzungsbedingungen, geändert durch Abschnitt 4(b) unten, gelten für Security Customer Success Services.

b. *Änderungsvereinbarungen*. Die Unterabschnitte 2(c) (Mandiant Consulting Services) und 2(f) (Weitere Definitionen) dieser Nutzungsbedingungen werden ausschließlich für Security Customer Success Services geändert wie folgt:

i. Verweise auf „Mandiant Consulting Services“ gelten jeweils als Verweise auf „Security Customer Success Services“.

ii. Unterabschnitt 2(c)(i) (Bereitstellung von Mandiant Consulting Services) wird folgendermaßen geändert:

Bereitstellung von Security Customer Success Services. Google erbringt die im Bestellformular angegebenen Security Customer Success Services, einschließlich der Liefergegenstände (sofern zutreffend), für den Kunden, vorausgesetzt, der Kunde kommt seinen Verpflichtungen gemäß Unterabschnitt 2(c)(v) (Verpflichtungen des Kunden) nach. Der Kunde darf Security Customer Success Services gemäß der Vereinbarung und der jeweiligen Dokumentation ausschließlich für interne Geschäftszwecke nutzen, und sofern er einen etwaigen Scope of Use einhält und alle Gebühren bezahlt wurden. Etwaige Liefergegenstände gelten als abgeschlossen, wenn der Kunde ihre Abnahme schriftlich oder mündlich bestätigt, oder zehn (10) Arbeitstage, nachdem

Google sie dem Kunden zur Verfügung gestellt hat, je nachdem, was zuerst eintritt. Security Customer Success Services umfassen keine Schulungsdienste.

iii. Die folgenden Bestimmungen in Unterabschnitt 2(c) finden keine Anwendung auf Security Customer Success Services und werden gelöscht: Unterabschnitt 2(c)(vii) (Gewährleistung und Rechtsbehelfe), Unterabschnitt 2(c)(xi) (Keine Werbung) und Unterabschnitt 2(c)(xii) (Google Cloud-Dienstdaten).

iv. Die Definition von Liefergegenstände in Unterabschnitt 2(f) wird folgendermaßen geändert:

„*Liefergegenstände*“ bezeichnen das Arbeitsprodukt, das die von Google beauftragten Personen im Rahmen der Security Customer Success Services für den Kunden bereitstellen und das in einem Bestellformular unter Liefergegenstände (“Deliverables”) aufgeführt ist.

Partnerspezifische Nutzungsbedingungen

1. Änderung der Bedingungen. Die folgenden Änderungen an diesen dienstspezifischen Nutzungsbedingungen für SecOps finden Anwendung, wenn die Vereinbarung den Weiterverkauf oder die Bereitstellung von SecOps-Diensten im Rahmen eines Google Cloud-Partner- oder -Reseller-Programms zulässt:

(a) Der Absatz dieser dienstspezifischen Nutzungsbedingungen für SecOps unter „Generative KI-Funktionen“ mit dem Titel „Einschränkungen“ wird folgendermaßen geändert:

Die in den oben genannten Absätzen (g) und (h) aufgeführten Einschränkungen sind „Nutzungseinschränkungen“ im Sinne des unter der Vereinbarung vereinbarten Google Cloud Platform Product Schedules.

(b) Absatz (b) dieser dienstspezifischen Nutzungsbedingungen für SecOps unter „Google Threat Intelligence und VirusTotal (GTI)“ wird geändert, indem der letzte Satz gelöscht und durch folgenden ersetzt wird:

Die in Absatz (b) aufgeführten Einschränkungen sind „Nutzungseinschränkungen“ im Sinne des unter der Vereinbarung vereinbarten Google Cloud Platform Product Schedules.

(c) Absatz (h)(ii) dieser dienstspezifischen Nutzungsbedingungen für SecOps unter „Google Threat Intelligence und VirusTotal (GTI)“ wird geändert, indem der letzte Satz gelöscht und durch folgenden ersetzt wird:

Die in Absatz (h)(ii) aufgeführten Einschränkungen sind „Nutzungseinschränkungen“ im Sinne des unter der Vereinbarung vereinbarten Google Cloud Platform Product Schedules.

2. Softwarebedingungen für Partner. Folgende Bestimmungen gelten für die Nutzung von Software (einschließlich „Premium-Software“ gemäß Definition in den allgemeinen Dienstbedingungen) durch den Partner:

(a) Unterlizenzen.

(i) Der Partner darf Software unterlizenzieren, aber nur an eigene Kunden, die die Software vom Partner beziehen („Autorisierte Unterlizenznehmer“).

(ii) Der Partner darf autorisierten Unterlizenznehmern nicht gestatten, Software weiter unterzulizenzieren.

(b) Einschränkungen bei der Bereitstellung. Sofern Google keine anderslautenden spezifischen schriftlichen Anweisungen gegeben hat, darf der Partner die Software nicht direkt für Dritte (einschließlich autorisierter Unterlizenznehmer) bereitstellen und muss autorisierte Unterlizenznehmer anweisen, die Software direkt über eine URL oder ein anderes von Google bereitgestelltes Repository herunterzuladen.

3. Partnerlizenzierte SKUs für die GTI-Einbindung. Wenn der Partner über ein Bestellformular SKUs für die GTI-Einbindung im Zusammenhang mit einem Kunden des Partners bestellt, der gemäß der Ausnahme „Partner-lizenzierte Managed Security Services-Kunden“ unter https://cloud.google.com/terms/direct-tos-exemptions?e=48754805&hl=pt-br) ausgenommen ist, dann:

(a) entspricht die Bezeichnung „Kundenprodukt(e)“ der Bezeichnung „Partnerprodukt(e)“, wodurch ein Angebot bezeichnet wird, das der Partner mit GTI oder wie im Bestellformular angegeben verbessert oder produziert. „Partnerprodukt“ beinhaltet nicht GTI.

(b) entspricht die Bezeichnung „Endnutzer von Kundenprodukten“ der Bezeichnung „Endnutzer von Partnerprodukten“, wodurch eine dritte Person oder Entität bezeichnet wird, die mit dem Partnerprodukt beziehungsweise den Partnerprodukten interagiert und das Kundenprodukt nur verwenden darf, um ihre eigenen internen Mitarbeiter, Daten, Systeme, Netzwerke, Anwendungen, Nutzer und Prozesse zu schützen.

(c) bezeichnet Endnutzervereinbarung eine Vereinbarung zwischen dem Partner und einem Endnutzer von Partnerprodukten, gemäß der der Partner Partnerprodukte verkauft oder liefert.

Nutzungsbedingungen der Google Cloud Platform

Sofern in einem Bestellformular oder einem Amendment nichts anderes vereinbart ist, gelten die Bestimmungen in diesem Abschnitt, wenn Google dem Kunden SecOps-Dienste gemäß einem Google Cloud Platform Services Schedule unter einem Cloud Master Agreement oder einer Google Cloud Platform-Lizenzvereinbarung („GCPLA“) (zusammenfassend als „GCP-Bedingungen“ bezeichnet) bereitstellt. In solchen Fällen sind die Bestimmungen in diesem Abschnitt Bestandteil der GCP-Bedingungen und regeln die Bereitstellung und Nutzung von SecOps-Diensten. Zur Klarstellung: Dieser Abschnitt gilt nicht für Google Cloud Platform-Dienste.

1. Geänderte Nutzungsbedingungen. Ausschließlich in Bezug auf SecOps-Dienste werden die GCP-Bedingungen folgendermaßen geändert:

   a. Die Abschnitte „Konten“ und „Admin-Konsole“ beziehungsweise der Abschnitt „Konto; Admin-Konsole“ werden folgendermaßen geändert:

      Konto. Google stellt dem Kunden das Konto bereit, über das dieser auf die Dienste zugreifen kann. Der Kunde ist verantwortlich für (a) die Sicherstellung der Vertraulichkeit und Sicherheit des Kontos, der zugehörigen Passwörter sowie der Google-API-Schlüssel und (b) jegliche Nutzung des Kontos.

   b. Der Abschnitt „Kündigung früherer Vereinbarungen“ (soweit vereinbart) wird folgendermaßen geändert:

      Kündigung früherer Vereinbarungen. Falls Google oder ein verbundenes Unternehmen von Google und der Kunde zuvor eine andere Vereinbarung über die Bereitstellung der Dienste geschlossen haben, endet diese zum Startdatum der Dienste. Die vorliegende Vereinbarung gilt künftig für die Bereitstellung und Nutzung der Dienste.

   c. Die Definition von „Konto“ wird folgendermaßen geändert:

„Konto“ bezeichnet das SecOps-Dienstkonto des Kunden.

d. Die Definition von „Kundendaten“ wird folgendermaßen geändert:

„Kundendaten“ bezeichnet (i) Daten, die der Kunde oder die Endnutzer Google über das Konto in den Diensten bereitstellen, sowie Daten, die der Kunde oder die Endnutzer durch die Nutzung der SecOps-Dienste aus diesen Daten ableiten, oder (ii) nur im Falle von Mandiant Consulting Services und Mandiant Managed Services Daten, die der Kunde oder die Endnutzer Google im Zusammenhang mit dem Erhalt der Dienste bereitstellen.

e. Die Definition von „Preise“ wird folgendermaßen geändert:

„Preise“ bezeichnet die Preise für die SecOps-Dienste, Software und technischen Supportdienste, wie in einem Bestellformular oder einer Amendment zur dienstspezifischen Anlage vereinbart.

2. GCPLA-Nutzungsbedingungen. Zusätzlich zu den Änderungen in Unterabschnitt 1 (Geänderte Nutzungsbedingungen) gelten die folgenden Änderungen nur für SecOps-Dienste, die im Rahmen einer Google Cloud Platform-Lizenzvereinbarung erworben werden:

a. Der Abschnitt „Verwendung von Kundendaten“ wird folgendermaßen geändert:

Verwendung von Kundendaten. Der Zugriff auf sowie die Verwendung und Verarbeitung von Kundendaten durch Google erfolgen ausschließlich gemäß dem Zusatz zur Verarbeitung von Cloud-Daten und niemals zu einem anderen Zweck. Google hat technische, organisatorische und physische Sicherheitsmaßnahmen zum Schutz der Kundendaten implementiert und wird diese aufrechterhalten. Eine nähere Beschreibung findet sich im Zusatz zur Verarbeitung von Cloud-Daten.

b. Der Abschnitt „Nutzung und Rechnungsstellung“ wird folgendermaßen geändert:

Nutzung und Rechnungsstellung. Der Kunde zahlt alle Gebühren für die Dienste sowie für die technischen Supportdienste. Detaillierte Nutzungsdaten werden von Google bereitgestellt, damit der Kunde die erworbene Dienste und die zugehörigen Gebühren nachprüfen kann. Sofern nichts Gegenteiliges in der Vereinbarung festgelegt wurde oder gesetzlich vorgeschrieben ist, sind die Gebühren für Dienste nicht erstattungsfähig.

3. Nicht anwendbare GCP-Nutzungsbedingungen. Die folgenden in den GCP-Nutzungsbedingungen definierten Bedingungen gelten nicht für SecOps-Dienste: „Admin-Konsole“, „Kundenanwendung“, „Anwendung“, „Dokumentation“, „Instanz“ und „Projekt“.

4. Erläuterungen und Zusatzinformationen zu SecOps. Die folgenden Bedingungen enthalten Erläuterungen und Zusatzinformationen hinsichtlich der Anwendung der GCP-Nutzungsbedingungen auf SecOps-Dienste:

a. Datenstandort: Bestimmungen in den GCP-Nutzungsbedingungen in Bezug auf den „Datenstandort“ gelten nicht für SecOps-Dienste. Der Datenstandort für SecOps-Dienste wird stattdessen durch Abschnitt 1.b (Standort) der allgemeinen Dienstbedingungen oben geregelt.

b. Wiederherstellungsziele (RTOs/RPOs): In den GCP-Nutzungsbedingungen genannte Recovery Time Objectives oder Recovery Point Objectives (RTOs/RPOs) gelten nicht für SecOps-Dienste.

c. Compliance-Zertifizierungen und SOC-Berichte: Ungeachtet anderer Bestimmungen in den GCP-Nutzungsbedingungen hinsichtlich Compliance-Zertifizierungen und Berichten erhält Google für SecOps-Dienste die unter https://cloud.google.com/security/compliance/secops/services-in-scope?hl=en genannten Zertifizierungen aufrecht und erstellt die dort aufgeführten Berichte. Google kann jederzeit Standards hinzufügen und eine Compliance-Zertifizierung oder einen SOC-Bericht durch eine gleichwertige oder bessere Alternative ersetzen.

d. Zusatz zur Verarbeitung von Cloud-Daten: Google verarbeitet Kundendaten gemäß der Vereinbarung, einschließlich des Zusatzes zur Verarbeitung von Cloud-Daten.

Vorherige Versionen *(zuletzt geändert am 1. Juli 2025)*

10. April 2025

30. Januar 2025

30. Oktober 2024

5. September 2024

15. Juli 2024

23. Mai 2024

4. April 2024