

Zusatz zur Verarbeitung von Cloud-Daten (Kunden)

Dieser Zusatz zur Verarbeitung von Cloud-Daten, einschließlich seiner Anhänge (der „Zusatz“), ist Bestandteil der Vereinbarung (wie unten definiert) zwischen Google und dem Kunden. Dieser Zusatz hieß zuvor „Bedingungen zur Datenverarbeitung und Sicherheitsbestimmungen“ (engl.: „Data Processing and Security Terms“) für die Google Cloud Platform, Looker (Original), Google SecOps-Dienste oder Google Cloud Skills Boost für Organisationen, „Zusatz zur Datenverarbeitungsvereinbarung“ (engl.: „Data Processing Amendment“) für Google Workspace oder Cloud Identity, und „Zusatz zur Datenverarbeitung“ (engl.: „Data Processing Addendum“) im Rahmen einer Vereinbarung für Mandiant Consulting Services und Managed Services.

Allgemeine Bedingungen

1. Überblick

In diesem Zusatz werden die Verpflichtungen der Parteien im Hinblick auf die Verarbeitung und Sicherheit von Kundendaten (wie unten definiert) gemäß den anwendbaren Gesetzen über Datensicherheit und Datenschutz beschrieben. Dieser Zusatz tritt ab dem Datum des Inkrafttretens des Zusatzes (wie unten definiert) in Kraft und ersetzt alle zuvor anwendbaren Bestimmungen zur Verarbeitung und zum Schutz von Kundendaten. Großgeschriebene Begriffe, die in diesem Zusatz verwendet, aber nicht definiert werden, haben die ihnen in der Vereinbarung zugewiesene Bedeutung.

2. Definitionen

2.1 In diesem Zusatz gelten folgende Definitionen:

- „Datum des Inkrafttretens des Zusatzes“ bezeichnet das Datum, an dem der Kunde diesen Zusatz akzeptiert hat oder die Parteien ihn auf andere Weise vereinbart haben.
- „Zusätzliche Sicherheitskontrollmaßnahmen“ bezeichnet Sicherheitsressourcen, Features, Funktionen und Kontrollen, die der Kunde nach eigenem Ermessen und eigener Entscheidung verwenden kann, einschließlich der Admin-Konsole, Verschlüsselung, Logging und Monitoring, Identitäts- und Zugriffsverwaltung, Sicherheitsscans und Firewalls.
- „Vereinbarung“ bezeichnet den Vertrag, unter dem Google sich verpflichtet hat, die betreffenden Dienste für den Kunden bereitzustellen.
- Der Begriff „Anwendbares Datenschutzrecht“ bezeichnet alle nationalen, bundesstaatlichen, EU-, Landes-, Provinz- oder sonstigen Gesetze oder Vorschriften zum Datenschutz und zur Datensicherheit, soweit sie auf die Verarbeitung personenbezogener Kundendaten anwendbar

sind. Zur Klarstellung: Anwendbare Datenschutzgesetze umfassen unter anderem die in Anhang 3 (Spezifische Datenschutzgesetze) genannten Gesetze, sind aber nicht auf diese beschränkt.

- „Geprüfte Dienste“ bezeichnet die jeweils aktuellen Dienste, die unter <https://cloud.google.com/security/compliance/services-in-scope> als in den Geltungsbereich der jeweiligen Zertifizierung oder des jeweiligen Berichts fallend aufgeführt sind. Google darf Dienste nicht aus dieser Liste (URL) entfernen, sofern sie nicht in Übereinstimmung mit der anwendbaren Vereinbarung eingestellt wurden.
- „Compliance-Zertifizierungen“ hat die in Abschnitt 7.4 (Compliance-Zertifizierungen und SOC-Berichte) angegebene Bedeutung.
- „Kundendaten“, falls nicht in der Vereinbarung definiert, hat die in Anhang 4 (Bestimmte Produkte) angegebene Bedeutung.
- „Personenbezogene Kundendaten“ bezeichnet die in den Kundendaten enthaltenen personenbezogenen Daten, einschließlich etwaiger besonderer Kategorien von personenbezogenen Daten oder sensibler Daten entsprechend der Definition im anwendbaren Datenschutzrecht.
- „Datenvorfall“ bezeichnet eine Verletzung der Sicherheit von Google, die zur versehentlichen oder unrechtmäßigen Zerstörung, zum versehentlichen oder unrechtmäßigen Verlust, zur versehentlichen oder unrechtmäßigen Veränderung, zur unbefugten Offenlegung oder zum unbefugten Zugriff auf Kundendaten auf Systemen führt, die von Google verwaltet oder anderweitig kontrolliert werden.
- „EMEA“ bezeichnet Europa, den Nahen Osten und Afrika.
- „EU-DSGVO“ bezeichnet die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.
- „Europäisches Datenschutzrecht“ bezeichnet, je nach Anwendbarkeit: (a) die DSGVO oder (b) das Schweizer Datenschutzgesetz (DSG).
- „Europäisches Recht“ bezeichnet, je nach Anwendbarkeit: (a) das Recht der EU oder eines EU-Mitgliedstaats (wenn die EU-DSGVO für die Verarbeitung personenbezogener Kundendaten gilt); (b) das Recht des Vereinigten Königreichs oder eines Teils des Vereinigten Königreichs (wenn die UK-DSGVO für die Verarbeitung personenbezogener Kundendaten gilt); oder (c) das Recht der Schweiz (wenn das Schweizer Datenschutzgesetz für die Verarbeitung personenbezogener Kundendaten gilt).
- „DSGVO“ bezeichnet je nach Anwendbarkeit: (a) die EU-DSGVO oder (b) die DSGVO des Vereinigten Königreichs (UK-DSGVO).

- „*Third-Party Auditor von Google*“ bezeichnet einen von Google ernannten, qualifizierten und unabhängigen externen Prüfer, dessen aktuelle Identität Google dem Kunden offenlegt.
- „*Weisungen*“ hat die in Abschnitt 5.2 beschriebene Bedeutung (Einhaltung der Weisungen des Kunden).
- „*Benachrichtigungs-E-Mail-Adresse*“ bezeichnet die E-Mail-Adresse(n), die der Kunde in der Admin-Konsole oder im Bestellformular angegeben hat, um bestimmte Benachrichtigungen von Google zu erhalten.
- „*Sicherheitsdokumentation*“ bezeichnet die Compliance-Zertifizierungen und SOC-Berichte.
- „*Sicherheitsmaßnahmen*“ hat die in Abschnitt 7.1.1 (Sicherheitsmaßnahmen von Google) angegebene Bedeutung.
- „*Dienste*“ bezeichnet die jeweiligen in Anhang 4 (Bestimmte Produkte) beschriebenen relevanten Dienste.
- „*SOC-Berichte*“ hat die in Abschnitt 7.4 (Compliance-Zertifizierungen und SOC-Berichte) angegebene Bedeutung.
- „*Unterauftragsverarbeiter*“ bezeichnet einen Dritten, der gemäß diesem Zusatz als weiterer Auftragsverarbeiter autorisiert ist, Kundendaten zu verarbeiten, um Teile der Dienste und TSD bereitzustellen (soweit anwendbar).
- „*Aufsichtsbehörde*“ bezeichnet je nach Anwendungsfall: (a) eine „Aufsichtsbehörde“ im Sinne der EU-DSGVO oder (b) den „Commissioner“ im Sinne der UK-DSGVO oder (c) den „Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten“ im Sinne des Schweizer DSG.
- „*Schweizer Datenschutzgesetz*“ bezeichnet, soweit anwendbar, das Bundesgesetz über den Datenschutz vom 19. Juni 1992 (Schweiz) (gemäß dem Bundesgesetz über den Datenschutz vom 14. Juni 1993) oder das überarbeitete Bundesgesetz über den Datenschutz vom 25. September 2020 (Schweiz) (gemäß dem Bundesgesetz über den Datenschutz vom 31. August 2022).
- „*Laufzeit*“ bezeichnet den Zeitraum vom Datum des Inkrafttretens des Zusatzes bis zum Ende der Bereitstellung der Dienste durch Google, einschließlich etwaiger Zeiträume, in denen die Bereitstellung der Dienste gesperrt sein kann und eines etwaigen Zeitraums nach der Beendigung, in dem Google die Dienste weiterhin für Übergangszwecke bereitstellen kann.
- „*UK-DSGVO*“ bezeichnet die EU-DSGVO in der geänderten und in das Recht des Vereinigten Königreichs übernommenen Fassung gemäß dem UK European Union (Withdrawal) Act 2018 sowie das jeweils anwendbare, unter diesem Act erlassene Sekundärrecht.

2.2 Die in diesem Zusatz verwendeten Begriffe „personenbezogene Daten“, „betroffene Person“, „Verarbeitung“, „Verantwortlicher“ und „Auftragsverarbeiter“ haben die im anwendbaren

Datenschutzrecht definierten Bedeutungen oder, wenn keine solche Bedeutung oder kein solches Gesetz vorliegt, die in der EU-DSGVO angegebenen Bedeutungen.

2.3 Soweit durch das anwendbare Datenschutzrecht vorgeschrieben, umfassen die Begriffe „betroffene Person“, „Verantwortlicher“ und „Auftragsverarbeiter“ jeweils „Verbraucher“, „Unternehmen“ und „Dienstleister“.

3. Dauer

Dieser Zusatz bleibt ungeachtet des Ablaufs der geltenden Vereinbarung in Kraft und erlischt automatisch, wenn alle Kundendaten durch Google wie in diesem Zusatz beschrieben gelöscht werden.

4. Rollen; Einhaltung gesetzlicher Vorschriften

4.1 *Rollen der Vertragsparteien.* Google ist ein Auftragsverarbeiter der personenbezogenen Daten des Kunden und der Kunde ist, je nach Anwendungsfall, ein Verantwortlicher oder Auftragsverarbeiter dieser Daten.

4.2 *Informationen zur Datenverarbeitung.* Der Gegenstand und die Einzelheiten der Verarbeitung der personenbezogenen Kundendaten sind in Anhang 1 (Gegenstand und Details der Datenverarbeitung) beschrieben.

4.3 *Einhaltung von Gesetzen.* Jede Vertragspartei ist verpflichtet, in Bezug auf die Verarbeitung der personenbezogenen Kundendaten ihren Verpflichtungen gemäß dem anwendbaren Datenschutzrecht nachzukommen.

4.4 *Zusätzliche rechtliche Bestimmungen.* Soweit die Verarbeitung personenbezogener Kundendaten unter ein in Anhang 3 (Spezifische Datenschutzgesetze) beschriebenes anwendbares Datenschutzrecht fällt, gelten die entsprechenden Bestimmungen in Anhang 3 zusätzlich zu diesen allgemeinen Bedingungen und haben Vorrang wie in Abschnitt 14.1 (Anwendungsvorrang) beschrieben.

5. Datenverarbeitung

5.1 *Der Kunde als Auftragsverarbeiter.* Wenn der Kunde ein Auftragsverarbeiter ist, gilt:

a. Der Kunde garantiert fortlaufend, dass der jeweilige datenschutzrechtlich Verantwortliche Folgendes genehmigt:

i. die Weisungen;

ii. die Beauftragung von Google als weiteren Auftragsverarbeiter durch den Kunden; und

iii. die Beauftragung von Unterauftragsverarbeitern durch Google wie in Abschnitt 11 (Unterauftragsverarbeiter) beschrieben;

b. Der Kunde verpflichtet sich, alle von Google gemäß den Abschnitten 7.2.1 (Benachrichtigung über Vorfälle), 9.2.1 (Verantwortung für Anfragen) oder 11.4 (Möglichkeit zum Widerspruch gegen Unterauftragsverarbeiter) übermittelten Benachrichtigungen schnellstmöglich und unverzüglich an den jeweiligen datenschutzrechtlich Verantwortliche weiterzuleiten.

c. Der Kunde kann dem jeweiligen datenschutzrechtlich Verantwortlichen jegliche sonstige Informationen über die Standorte von Google-Rechenzentren oder die Namen, Standorte und Tätigkeitsbereiche von Unterauftragsverarbeitern bereitstellen, die von Google gemäß diesem Zusatz zur Verfügung gestellt werden.

5.2 Einhaltung der Weisungen des Kunden. Der Kunde weist Google an, die Kundendaten ausschließlich gemäß der geltenden Vereinbarung (einschließlich dieses Zusatzes) zu verarbeiten, um:

a. die Dienste und TSD bereitzustellen, abzusichern und zu überwachen (soweit anwendbar); und

b. wie näher spezifiziert durch:

i. die Nutzung der Dienste (einschließlich der Admin-Konsole) und der TSD durch den Kunden (soweit anwendbar); und

ii. wie zusätzlich in anderen schriftlichen Weisungen dokumentiert ist, die vom Kunden gegeben wurden und von Google förmlich als Weisung im Sinne des vorliegenden Zusatzes bestätigt wurden

(zusammen die „Weisungen“).

Google wird die Anweisungen befolgen, sofern dies nicht durch europäisches Recht, wo europäisches Datenschutzrecht gilt, oder durch geltendes Recht, wo andere geltende Datenschutzgesetze gelten, untersagt ist.

6. Löschen von Daten

6.1 Löschung durch den Kunden. Google wird es dem Kunden ermöglichen, Kundendaten während der Laufzeit in Übereinstimmung mit den Funktionen der Dienste zu löschen. Wenn der Kunde die Dienste nutzt, um Kundendaten während der geltenden Laufzeit zu löschen und diese Kundendaten vom Kunden nicht wiederhergestellt werden können, begründet diese Verwendung eine Anweisung an Google, die relevanten Kundendaten aus den Google-Systemen zu löschen. Google wird dieser Weisung Folge leisten, sobald dies vernünftigerweise möglich ist, spätestens aber innerhalb einer Höchstfrist von 180 Tagen, sofern nicht europäisches Recht, wo europäisches Datenschutzrecht gilt, oder anderes Recht, wo andere Datenschutzgesetze Anwendung finden, eine Aufbewahrung vorschreibt.

6.2 Rückgabe oder Löschung am Ende der Laufzeit. Wenn der Kunde Kundendaten nach dem Ablauf der Laufzeit behalten möchte, kann er Google gemäß Abschnitt 9.1 (Zugriff; Berichtigung; eingeschränkte Verarbeitung; Übertragbarkeit) anweisen, diese Daten während der Laufzeit zurückzugeben. Vorbehaltlich Abschnitt 6.3 (Aufgeschobene Löschanweisung) gilt: Der Kunde weist Google nach Ablauf der geltenden Laufzeit an, alle Kundendaten (einschließlich vorhandener Kopien) aus den Google-Systemen zu löschen. Nach einem Wiederherstellungszeitraum von bis zu 30 Tagen ab diesem Datum wird Google dieser Weisung Folge leisten, sobald dies vernünftigerweise möglich ist, spätestens aber innerhalb einer Höchstfrist von 180 Tagen, sofern nicht europäisches Recht, wo europäisches Datenschutzrecht gilt, oder anderes Recht, wo andere Datenschutzgesetze Anwendung finden, eine Aufbewahrung vorschreibt.

6.3 *Aufgeschobene Löschanweisung.* Soweit Kundendaten, die unter die in Abschnitt 6.2 (Rückgabe oder Löschung am Ende der Laufzeit) beschriebene Löschanweisung fallen, bei Ablauf der geltenden Laufzeit gemäß Abschnitt 6.2 ebenfalls verarbeitet werden in Bezug auf eine Vereinbarung mit noch fortlaufender Laufzeit, wird die Löschanweisung erst bei Ablauf der fortlaufenden Laufzeit wirksam. Zur Klarstellung: Dieser Nachtrag gilt weiterhin für diese Kundendaten, bis sie von Google gelöscht werden.

7. Datensicherheit

7.1 *Googles Sicherheitsmaßnahmen, Kontrollen und Unterstützung*

7.1.1 *Googles Sicherheitsmaßnahmen.* Google wird technische, organisatorische und physische Maßnahmen zum Schutz der Kundendaten vor versehentlicher oder unrechtmäßiger Zerstörung, Verlust, Veränderung, unbefugter Offenlegung oder unbefugtem Zugriff gemäß Anhang 2 (Sicherheitsmaßnahmen) (die „**Sicherheitsmaßnahmen**“) implementieren und aufrechterhalten. Die Sicherheitsmaßnahmen umfassen Maßnahmen zur Verschlüsselung von Kundendaten, zur Gewährleistung der fortlaufenden Vertraulichkeit, Integrität, Verfügbarkeit und Ausfallsicherheit der Systeme und Dienste von Google, zur zeitnahen Wiederherstellung des Zugriffs auf Kundendaten nach einem Vorfall sowie zur regelmäßigen Überprüfung der Wirksamkeit. Google kann die Sicherheitsmaßnahmen von Zeit zu Zeit aktualisieren, sofern diese Aktualisierungen nicht zu einer wesentlichen Verringerung der Sicherheit der Dienste führen.

7.1.2 *Zugriff und Compliance.* Google wird:

- a. seinen Mitarbeitern, Auftragnehmern und Unterauftragsverarbeitern den Zugriff auf personenbezogene Kundendaten nur in dem Maß gestatten, wie es zur Erfüllung der Weisungen unbedingt erforderlich ist;
- b. geeignete Schritte unternehmen, um die Einhaltung der Sicherheitsmaßnahmen durch seine Mitarbeiter, Auftragnehmer und Unterauftragsverarbeiter sicherzustellen, soweit dies für deren Leistungsumfang relevant ist; und
- c. gewährleisten, dass alle Personen, die zur Verarbeitung personenbezogener Kundendaten befugt sind, zur Vertraulichkeit verpflichtet sind.

7.1.3 *Zusätzliche Sicherheitskontrollmaßnahmen.* Google stellt zusätzliche Sicherheitskontrollmaßnahmen zur Verfügung, um:

- a. dem Kunden zu ermöglichen, Maßnahmen zum Schutz der Kundendaten zu ergreifen; und
- b. dem Kunden Informationen über den Schutz, den Zugriff auf und die Nutzung der Kundendaten bereitzustellen.

7.1.4 *Sicherheitsunterstützung von Google.* Google wird (unter Berücksichtigung der Art der Verarbeitung personenbezogener Kundendaten und der Google zur Verfügung stehenden Informationen) den Kunden bei der Einhaltung seiner Verpflichtungen (oder, wenn der Kunde ein Auftragsverarbeiter ist, der Verpflichtungen des entsprechenden Verantwortlichen) in Bezug auf Sicherheit und Datenschutzverletzungen gemäß den jeweils geltenden Datenschutzgesetzen sicherzustellen, indem Google:

- a. die Sicherheitsmaßnahmen gemäß Abschnitt 7.1.1 (Sicherheitsmaßnahmen von Google) umsetzt und aufrechterhält;
- b. zusätzliche Sicherheitskontrollmaßnahmen gemäß Abschnitt 7.1.3 (Zusätzliche Sicherheitskontrollmaßnahmen) zur Verfügung stellt;
- c. die Bestimmungen von Abschnitt 7.2 (Datenvorfälle) einhält;
- d. die Sicherheitsdokumentation gemäß Abschnitt 7.5.1 (Überprüfung der Sicherheitsdokumentation) zur Verfügung stellt und die in der Vereinbarung (einschließlich dieses Nachtrags) enthaltenen Informationen bereitstellt; und
- e. wenn die vorstehenden Unterabschnitte (a) bis (d) für den Kunden (oder den entsprechenden datenschutzrechtlich Verantwortlichen) zur Erfüllung dieser Verpflichtungen nicht ausreichen, dem Kunden auf dessen Anfrage hin zusätzliche angemessene Zusammenarbeit und Unterstützung gewährt.

7.2 Datenvorfälle.

7.2.1 Meldung eines Vorfalls. Google benachrichtigt den Kunden schnellstmöglich und unverzüglich, nachdem Google von einem Datenvorfall erfahren hat, und ergreift umgehend angemessene Schritte, um Schäden zu minimieren und Kundendaten zu schützen.

7.2.2 Details zu Datenvorfällen. Die Benachrichtigungen von Google über den Datenvorfall enthalten folgende Informationen: die Art des Datenvorfalls, einschließlich der betroffenen Kundenressourcen; die Maßnahmen, die Google getroffen hat oder zu treffen beabsichtigt, um den Datenvorfall zu beheben und die damit verbundene potenzielle Gefahr einzudämmen; die Maßnahmen, die Google gegebenenfalls dem Kunden empfiehlt, um den Datenvorfall zu beheben; und Angaben einer Kontaktstelle, bei der weitere Informationen eingeholt werden können. Wenn es nicht möglich ist, alle diese Informationen zur selben Zeit zur Verfügung zu stellen, enthält die erste Benachrichtigung von Google die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden unverzüglich bereitgestellt, sobald sie verfügbar sind.

7.2.3 Keine Auswertung von Kundendaten durch Google. Google ist nicht verpflichtet, Kundendaten auszuwerten, um Informationen zu identifizieren, die bestimmten rechtlichen Anforderungen unterliegen.

7.2.4 Keine Anerkennung eines Verschuldens durch Google. Die Benachrichtigung oder Reaktion von Google auf einen Datenvorfall gemäß diesem Abschnitt 7.2 (Datenvorfälle) ist kein Anerkenntnis oder Zugeständnis eines Verschuldens oder einer Haftung seitens Google in Bezug auf den Datenvorfall.

7.3 Sicherheitsverantwortlichkeiten und -bewertung des Kunden.

7.3.1 Sicherheitspflichten des Kunden. Unbeschadet der Verpflichtungen von Google gemäß Abschnitt 7.1 (Sicherheitsmaßnahmen, Kontrollen und Unterstützung durch Google) und 7.2 (Datenvorfälle) sowie anderen Bestimmungen der Vereinbarung ist der Kunde für die Nutzung der Dienste und die

Speicherung von Kopien der Kundendaten außerhalb der Systeme von Google oder von Unterauftragsverarbeitern von Google verantwortlich. Darunter fallen:

- a. die Nutzung der Dienste und zusätzlichen Sicherheitskontrollmaßnahmen, um ein dem Risiko in Bezug auf die Kundendaten angemessenes Sicherheitsniveau zu gewährleisten;
- b. die Sicherung der Anmeldedaten, Systeme und Geräte zur Kontoauthentifizierung, die der Kunde für den Zugriff auf die Dienste verwendet; und
- c. gegebenenfalls die Sicherung oder Aufbewahrung von Kopien der Kundendaten.

7.3.2 Sicherheitsbewertung des Kunden. Der Kunde erklärt sich damit einverstanden, dass die Dienste, Sicherheitsmaßnahmen, zusätzlichen Sicherheitskontrollmaßnahmen und Verpflichtungen von Google gemäß diesem Abschnitt 7 (Datensicherheit) ein Sicherheitsniveau bieten, das dem Risiko für die Kundendaten angemessen ist (unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung der Kundendaten sowie der Risiken für natürliche Personen).

7.4 Compliancezertifizierungen und SOC-Berichte. Google behält für die geprüften Dienste mindestens Folgendes bei, um die anhaltende Wirksamkeit der Sicherheitsmaßnahmen zu belegen:

- a. Zertifikate für ISO 27001 und alle weiteren in Anhang 4 (Bestimmte Produkte) beschriebenen Zertifizierungen (die „*Compliance-Zertifizierungen*“); und
- b. SOC 2- und SOC 3-Berichte, die durch den externen Prüfer von Google erstellt und jährlich auf der Grundlage eines mindestens alle 12 Monate durchgeführten Audits aktualisiert werden (die „*SOC-Berichte*“).

Google kann jederzeit Standards hinzufügen. Google kann eine Compliance-Zertifizierung oder einen SOC-Bericht durch eine gleichwertige oder verbesserte Alternative ersetzen.

7.5 Überprüfungen und Compliance-Audits.

7.5.1 Überprüfungen der Sicherheitsdokumentation. Um die Einhaltung seiner Verpflichtungen gemäß diesem Zusatz nachzuweisen, stellt Google dem Kunden die Sicherheitsdokumentation zur Überprüfung zur Verfügung und gestattet dem Kunden, sofern dieser ein Auftragsverarbeiter ist, gemäß Abschnitt 7.5.3 (Zusätzliche Geschäftsbedingungen für Überprüfungen und Audits) Zugang zu den SOC-Berichten für den jeweiligen datenschutzrechtlich Verantwortlichen zu verlangen.

7.5.2 Audit-Rechte des Kunden.

- a. *Vom Kunden durchgeführte Audits.* Sofern gemäß anwendbarem Datenschutzrecht erforderlich, gestattet Google dem Kunden oder einem vom Kunden beauftragten unabhängigen Prüfer, nach näherer Maßgabe des Abschnitts 7.5.3 (Zusätzliche Geschäftsbedingungen für Überprüfungen und Audits) Audits (einschließlich Inspektionen) durchzuführen, um zu überprüfen, ob Google seine Verpflichtungen aus diesem Zusatz einhält. Während eines Audits arbeitet Google wie in Abschnitt 7.5 (Überprüfungen und

Compliance-Audits) beschrieben in angemessener Weise mit dem Kunden oder dem von ihm beauftragten Prüfer zusammen.

b. *Unabhängige Prüfung durch Kunden.* Der Kunde kann einen Audit durchführen, um die Einhaltung der Verpflichtungen von Google gemäß diesem Zusatz zu überprüfen, indem er die Sicherheitsdokumentation (die die Ergebnisse der durch den Third Party Auditor von Google durchgeführten Prüfungen widerspiegelt) überprüft.

7.5.3 Zusätzliche Geschäftsbedingungen für Überprüfungen und Audits.

a. Der Kunde muss sich an das Cloud-Datenschutzteam wenden, um Folgendes anzufordern:

i. Zugriff auf die SOC-Berichte für den jeweiligen datenschutzrechtlich Verantwortlichen gemäß Abschnitt 7.5.1 (Überprüfung der Sicherheitsdokumentation) oder

ii. einen Audit gemäß Abschnitt 7.5.2(a) (Vom Kunden durchgeführte Audits).

b. Nach einer Anfrage des Kunden gemäß Abschnitt 7.5.3(a) werden Google und der Kunde im Voraus Folgendes besprechen und vereinbaren:

i. Sicherheits- und Vertraulichkeitskontrollmaßnahmen, die für jeden Zugriff auf die SOC-Berichte durch einen datenschutzrechtlich Verantwortlichen Dritten gemäß Abschnitt 7.5.1 (Überprüfung der Sicherheitsdokumentation) gelten; und

ii. das angemessene Startdatum, den Umfang und die Dauer sowie die Sicherheits- und Vertraulichkeitskontrollmaßnahmen, die für jeden Audit gemäß Abschnitt 7.5.2(a) (Vom Kunden durchgeführte Audits) gelten.

c. Google kann für jeden Audit gemäß Abschnitt 7.5.2(a) (Vom Kunden durchgeführte Audits) eine Gebühr (basierend auf den angemessenen Kosten von Google) erheben. Google wird dem Kunden vor einem solchen Audit weitere Einzelheiten zu allen anfallenden Gebühren und deren Berechnungsgrundlage mitteilen. Der Kunde ist für alle Gebühren verantwortlich, die von einem vom Kunden mit der Durchführung eines solchen Audits beauftragten Prüfer erhoben werden.

d. Google kann einem vom Kunden für Audits gemäß Abschnitt 7.5.2(a) (Vom Kunden durchgeführte Audits) beauftragten Prüfer schriftlich widersprechen, wenn Google berechtigten Grund zu der Annahme hat, dass der Prüfer nicht angemessen qualifiziert oder unabhängig ist, oder es sich um einen Wettbewerber von Google handelt oder der Prüfer anderweitig erkennbar ungeeignet ist. Ein solcher Widerspruch von Google verpflichtet den Kunden, einen anderen Prüfer zu benennen oder den Audit selbst durchzuführen.

e. Alle Kundenanfragen gemäß Anhang 3 (Spezifische Datenschutzgesetze) oder Anhang 4 (Bestimmte Produkte) bezüglich des Zugriffs auf SOC-Berichte für einen datenschutzrechtlich verantwortlichen Dritten oder für Audits unterliegen ebenfalls diesem Abschnitt 7.5.3 (Zusätzliche Geschäftsbedingungen für Überprüfungen und Audits).

8. Folgenabschätzungen und Konsultationen

Google wird (unter Berücksichtigung der Art der Verarbeitung und der Google zur Verfügung stehenden Informationen) den Kunden bei der Einhaltung seiner Verpflichtungen (oder, wenn der Kunden ein Auftragsverarbeiter ist, der Verpflichtungen des datenschutzrechtlich verantwortlichen Dritten) in Bezug auf Datenschutz-Folgenabschätzungen, Risikobewertungen, vorherige Konsultationen der Datenschutzaufsichtsbehörde oder entsprechende Verfahren gemäß den jeweils geltenden Datenschutzgesetzen sicherzustellen, indem Google:

- a. zusätzliche Sicherheits Kontrollmaßnahmen gemäß Abschnitt 7.1.3 (Zusätzliche Sicherheitskontrollmaßnahmen) und die Sicherheitsdokumentation gemäß Abschnitt 7.5.1 (Überprüfungen der Sicherheitsdokumentation) bereitstellt;
- b. die in dieser Vereinbarung (einschließlich dieses Zusatzes) enthaltenen Informationen bereitstellt; und,
- c. wenn die vorstehenden Unterabschnitte (a) und (b) zur Erfüllung dieser Verpflichtungen des Kunden (oder des datenschutzrechtlich verantwortlichen Dritten) nicht ausreichen, dem Kunden auf dessen Anfrage hin zusätzliche angemessene Zusammenarbeit und Unterstützung gewährt.

9. Zugriff; Rechte betroffener Personen; Datenexport

9.1 Zugriff; Berichtigung; Einschränkung der Verarbeitung; Portabilität. Während der Laufzeit ermöglicht Google dem Kunden in einer Weise, die mit der Funktionalität der Dienste vereinbar ist, den Zugriff auf Kundendaten, deren Berichtigung und die Einschränkung ihrer Verarbeitung, einschließlich über die von Google bereitgestellte Löschfunktion, wie in Abschnitt 6.1 (Löschung durch den Kunden) beschrieben, sowie den Export von Kundendaten. Stellt der Kunde fest, dass personenbezogene Kundendaten unrichtig oder veraltet sind, ist er dafür verantwortlich, diese Daten mithilfe dieser Funktion zu berichtigen oder zu löschen, sofern dies nach den geltenden Datenschutzgesetzen erforderlich ist.

9.2 Betroffenenanfragen

9.2.1 Verantwortung für die Bearbeitung von Anfragen. Wenn das Cloud-Datenschutzteam von Google während der Laufzeit eine Anfrage von einer betroffenen Person erhält, die sich auf personenbezogene Daten des Kunden bezieht und den Kunden identifiziert, wird Google:

- a. die betroffene Person auffordern, ihre Anfrage an den Kunden zu richten;
- b. den Kunden unverzüglich benachrichtigen; und
- c. ohne Zustimmung des Kunden nicht anderweitig auf die Anfrage der betroffenen Person reagieren.

Der Kunde ist für die Beantwortung solcher Anfragen verantwortlich, gegebenenfalls unter Verwendung der Funktionen der Dienste.

9.2.2 Unterstützung durch Google bei Anfragen betroffener Personen. Google unterstützt den Kunden (unter Berücksichtigung der Art der Verarbeitung der personenbezogenen Kundendaten) bei der

Erfüllung seiner, gemäß des jeweils anwendbaren Datenschutzrechts bestehenden Verpflichtungen (oder, wenn der Kunden ein Auftragsverarbeiter ist, der Verpflichtungen des dritten datenschutzrechtlich Verantwortlichen), Betroffenenanfragen zu beantworten, indem Google:

- a. zusätzliche Sicherheitskontrollmaßnahmen gemäß Abschnitt 7.1.3 (Zusätzliche Sicherheitskontrollmaßnahmen) bereitstellt;
- b. die Abschnitte 9.1 (Zugriff, Berichtigung, Einschränkung der Verarbeitung, Portabilität) und 9.2.1 (Verantwortung für die Bearbeitung von Anfragen) einhält und,
- c. wenn die vorstehenden Unterabschnitte (a) und (b) zur Erfüllung dieser Verpflichtungen des Kunden (oder des datenschutzrechtlich verantwortlichen Dritten) nicht ausreichen, dem Kunden auf dessen Anfrage hin zusätzliche angemessene Zusammenarbeit und Unterstützung gewährt.

10. Orte der Datenverarbeitung

10.1 *Einrichtungen zur Datenspeicherung und -verarbeitung.* Vorbehaltlich der Verpflichtungen von Google hinsichtlich des Speicherorts von Daten gemäß den geltenden dienstspezifischen Nutzungsbedingungen und, falls anwendbar, hinsichtlich der Datenübermittlung gemäß Anhang 3 (Spezifische Datenschutzgesetze), können Kundendaten in jedem Land verarbeitet werden, in dem Google oder seine Unterauftragsverarbeiter Einrichtungen unterhalten.

10.2 *Informationen zu Rechenzentren.* Die Standorte der Google-Rechenzentren sind in Anhang 4 (Bestimmte Produkte) beschrieben.

11. Unterauftragsverarbeiter

11.1 *Zustimmung zum Einsatz von Unterauftragsverarbeitern.* Der Kunde erteilt Google die ausdrückliche Genehmigung, die zum Zeitpunkt des Inkrafttretens des Zusatzes gemäß Abschnitt 11.2 (Informationen zu Unterauftragsverarbeitern) benannten und beschriebenen Unternehmen als Unterauftragsverarbeiter einzusetzen. Darüber hinaus erteilt der Kunde unbeschadet des Abschnitts 11.4 (Möglichkeit zum Widerspruch gegen Unterauftragsverarbeiter) Google die allgemeine Genehmigung, Dritte als Unterauftragsverarbeiter („neue Unterauftragsverarbeiter“) zu beauftragen.

11.2 *Informationen zu Unterauftragsverarbeitern.* Namen, Standorte und Tätigkeitsbereiche der Unterauftragsverarbeiter werden in Anhang 4 (Bestimmte Produkte) beschrieben.

11.3 *Anforderungen an den Einsatz von Unterauftragsverarbeitern.* Beim Einsatz jedes Unterauftragsverarbeiters wird Google:

- a. durch einen schriftlichen Vertrag sicherstellen, dass:
 - i. der Unterauftragsverarbeiter nur in dem Umfang auf Kundendaten zugreift und diese nutzt, wie es zur Erfüllung der ihm übertragenen Verpflichtungen erforderlich ist, und dies in Übereinstimmung mit der Vereinbarung (einschließlich dieses Nachtrags) tut; und

ii. dem Unterauftragsverarbeiter die in diesem Nachtrag beschriebenen Datenschutzverpflichtungen auferlegt werden, sofern dies nach den geltenden Datenschutzgesetzen erforderlich ist (wie in Anhang 3 (Spezifische Datenschutzgesetze) ggfls. näher beschrieben); und

b. Google für alle dem Unterauftragsverarbeiter übertragenen Verpflichtungen sowie für alle Handlungen und Unterlassungen des Unterauftragsverarbeiters in vollem Umfang haftbar bleibt.

11.4 Möglichkeit, dem Einsatz eines Unterauftragsverarbeiters zu widersprechen.

a. Wenn Google während der Laufzeit einen neuen Unterauftragsverarbeiter einsetzt, wird Google den Kunden mindestens 30 Tage vor Beginn der Verarbeitung von Kundendaten durch den neuen Unterauftragsverarbeiter über dessen Einsatz (einschließlich des Namens, Standorts und Tätigkeiten des neuen Unterauftragsverarbeiters) informieren.

b. Der Kunde kann innerhalb von 90 Tagen nach Benachrichtigung über den Einsatz eines neuen Unterauftragsverarbeiters Widerspruch erheben, indem er die ordentliche Kündigung der Vereinbarung erklärt

i. gemäß den Regelungen in der Vereinbarung über eine ordentliche Kündigung der Vereinbarung; oder

ii. falls es in der Vereinbarung keine solche Regelung gibt, indem er Google von seiner Kündigung in Kenntnis setzt.

12. Cloud-Datenschutzteam; Verzeichnis von Verarbeitungstätigkeiten

12.1 *Cloud-Datenschutzteam.* Das Cloud-Datenschutzteam von Google leistet bei allen Anfragen des Kunden im Zusammenhang mit der Verarbeitung von Kundendaten gemäß der Vereinbarung umgehend und in angemessener Weise Unterstützung und kann wie im Abschnitt „Hinweise“ der Vereinbarung oder in Anhang 4 (Spezifische Produkte) beschrieben kontaktiert werden.

12.2 *Verzeichnis von Verarbeitungstätigkeiten von Google.* Google unterhält eine den Anforderungen der jeweils anwendbaren Datenschutzgesetze angemessene Dokumentation seiner Verarbeitungstätigkeiten. Soweit Google gemäß den jeweils anwendbaren Datenschutzgesetzen verpflichtet ist, bestimmte Informationen über den Kunden zu erfassen und aufzubewahren, nutzt der Kunde die Admin-Konsole oder andere in Anhang 4 (Spezifische Produkte) genannte Mittel, um diese Informationen bereitzustellen und sie korrekt und aktuell zu halten. Google kann diese Informationen den zuständigen Behörden, einschließlich einer Aufsichtsbehörde, zur Verfügung stellen, wenn dies nach dem jeweils anwendbaren Datenschutzrecht erforderlich ist.

12.3 *Anfragen durch den Verantwortlichen.* Wenn das Cloud-Datenschutzteam von Google während der Laufzeit eine Anfrage oder Anweisung von einem Dritten erhält, der sich als Verantwortlicher für personenbezogene Daten des Kunden ausgibt, wird Google den Dritten auffordern, sich an den Kunden zu wenden.

13. Mitteilungen

Mitteilungen unter diesem Zusatz (einschließlich Mitteilungen über Datenvorfälle) werden an die Benachrichtigungs-E-Mail-Adresse gesendet. Der Kunde ist dafür verantwortlich, die Admin-Konsole zu verwenden oder Google anderweitig zu benachrichtigen, um sicherzustellen, dass seine Benachrichtigungs-E-Mail-Adresse aktuell und gültig ist.

14. Auslegung

14.1 *Anwendungsvorrang*. Im Fall eines Widerspruchs

- a. zwischen Anhang 3 (Spezifische Datenschutzgesetze) und dem übrigen Zusatz (einschließlich Anhang 4 „Bestimmte Produkte“) hat Anhang 3 Vorrang.
- b. zwischen Anhang 4 (Bestimmte Produkte) und dem übrigen Zusatz (mit Ausnahme von Anhang 3) hat Anhang 4 Vorrang.
- c. zwischen diesem Zusatz und der übrigen Vereinbarung hat dieser Zusatz Vorrang.

14.2 *Verweise auf Abschnitte*. Sofern nicht anders angegeben, beziehen sich Verweise auf Abschnitte in allen Anhängen dieses Zusatzes auf die Abschnitte in den allgemeinen Bedingungen des Zusatzes.

Anhang 1: Gegenstand und Details der Datenverarbeitung

Gegenstand

Die Bereitstellung der Dienste und der TSD (soweit anwendbar) für den Kunden durch Google.

Dauer der Verarbeitung

Die Laufzeit zuzüglich des Zeitraums vom Ende der Laufzeit bis zum Löschen aller Kundendaten durch Google in Übereinstimmung mit diesem Zusatz.

Art und Zweck der Verarbeitung

Google verarbeitet personenbezogene Kundendaten zum Zweck der Bereitstellung der Dienste und der TSD (soweit anwendbar) für den Kunden gemäß diesem Zusatz.

Datenkategorien

Daten zu Personen, die Google über die Dienste vom (oder auf Anweisung des) Kunden oder von den Endnutzern des Kunden zur Verfügung gestellt werden.

Betroffene Personen

Zu den betroffenen Personen zählen die Personen, über die Google Daten über die Dienste vom (oder auf Anweisung des) Kunden oder von den Endnutzern des Kunden zur Verfügung gestellt werden.

Anhang 2: Sicherheitsmaßnahmen

Ab dem Datum des Inkrafttretens des Zusatzes implementiert Google die in diesem Anhang 2 aufgeführten Sicherheitsmaßnahmen und erhält sie aufrecht.

1. Rechenzentrums- und Netzwerksicherheit

(a) Rechenzentren.

Infrastruktur. Google unterhält geografisch verteilte Rechenzentren. Google speichert alle Produktionsdaten in physisch sicheren Rechenzentren.

Redundanz. Die Infrastruktursysteme wurden so konzipiert, dass Single Points of Failure eliminiert und die Auswirkungen vorhersehbarer Umweltrisiken minimiert werden. Doppelte Schaltkreise, Switches, Netzwerke oder andere erforderliche Geräte tragen dazu bei, diese Redundanz zu gewährleisten. Die Dienste sind so konzipiert, dass Google bestimmte Arten von vorbeugenden und korrektiven Wartungsarbeiten ohne Unterbrechung durchführen kann. Für alle Umweltausrüstungen und -einrichtungen gibt es dokumentierte vorbeugende Wartungsverfahren, in denen der Ablauf und die Häufigkeit der Durchführung gemäß den Herstellerangaben oder internen Spezifikationen detailliert beschrieben sind. Die vorbeugende und korrektive Wartung der Ausrüstung des Rechenzentrums wird durch einen standardisierten Änderungsprozess gemäß den dokumentierten Verfahren terminiert.

Stromversorgung. Die Stromversorgungssysteme der Rechenzentren sind redundant ausgelegt und können ohne Beeinträchtigung des Dauerbetriebs rund um die Uhr (24 Stunden am Tag und 7 Tage die Woche) gewartet werden. In den meisten Fällen wird für kritische Infrastrukturkomponenten im Rechenzentrum eine primäre und eine alternative Stromquelle mit jeweils gleicher Kapazität bereitgestellt. Die Notstromversorgung erfolgt über verschiedene Mechanismen, z. B. durch unterbrechungsfreie Stromversorgungsbatterien (USV), die bei partiellen Stromausfällen, Stromausfällen, Überspannung, Unterspannung und Frequenz-Toleranzüberschreitungen eine durchgängig zuverlässige Stromabsicherung ermöglichen. Falls die Stromversorgung des Energieversorgers unterbrochen wird, ist die Ersatzversorgung so ausgelegt, dass die Rechenzentren übergangsweise bei voller Last Energie für bis zu 10 Minuten erhalten, bis die Notstromgeneratoren die Versorgung übernehmen. Die Notstromgeneratoren sind in der Lage, automatisch innerhalb von Sekunden hochzufahren und genügend Notstrom bereitzustellen, um das Rechenzentrum in der Regel über einen Zeitraum von Tagen bei voller Kapazität zu betreiben.

Server-Betriebssysteme. Google-Server verwenden eine Linux-basierte Implementierung, die an die Anwendungsumgebung angepasst ist. Die Daten werden mit proprietären Algorithmen gespeichert, um die Datensicherheit und Redundanz zu erhöhen.

Codequalität. Google verwendet einen Prozess zur Code Review, um die Sicherheit des Codes für die Bereitstellung der Dienste zu erhöhen und die Sicherheitsprodukte in Produktionsumgebungen zu verbessern.

Aufrechterhaltung des Betriebs. Google hat Notfallpläne zur Aufrechterhaltung des Geschäftsbetriebes und Programme zur Notfallwiederherstellung konzipiert, die regelmäßig weiterentwickelt und getestet werden.

(b) Netzwerke und Übertragung.

Datenübertragung. Rechenzentren sind in der Regel über private Hochgeschwindigkeitsverbindungen vernetzt, um eine sichere und schnelle Datenübertragung zwischen Rechenzentren zu gewährleisten. Dies soll verhindern, dass Daten während der elektronischen Übertragung oder des Transports oder während der Aufzeichnung auf Datenträger ohne Autorisierung gelesen, kopiert, geändert oder entfernt werden. Google überträgt Daten über Internet-Standardprotokolle.

Externe Angriffsfläche. Google unterhält mehrere Layer von Netzwerkgeräten und Systemen zur Einbruchserkennung, um die externe Angriffsfläche abzusichern. Google zieht potenzielle Angriffsvektoren in Betracht und integriert angemessene, speziell entwickelte Technologien in von außen erreichbare Systeme.

Intrusion Detection. Intrusion Detection soll Einblicke in laufende Angriffsaktivitäten geben und angemessene Informationen für die Reaktion auf Vorfälle liefern. Die Intrusion Detection von Google umfasst: (i) die strenge Kontrolle der Größe und Zusammensetzung der Angriffsfläche von Google durch vorbeugende Maßnahmen; (ii) den Einsatz intelligenter Erkennungskontrollen an Dateneingabepunkten; und (iii) den Einsatz von Technologien, die bestimmte gefährliche Situationen automatisch beheben.

Incident Response. Google überwacht eine Vielzahl von Kommunikationskanälen auf Sicherheitsvorfälle und das Sicherheitspersonal von Google reagiert umgehend auf bekannte Vorfälle.

Verschlüsselungstechnologien. Google stellt HTTPS-Verschlüsselung (auch als SSL- oder TLS-Verbindung bezeichnet) zur Verfügung. Google-Server unterstützen einen Austausch von RSA- und ECDSA-signierten Schlüsseln nach Diffie-Hellman auf Basis sitzungsspezifischer Elliptische-Kurven-Kryptografie. Diese PFS-Methoden (Perfect Forward Secrecy) tragen dazu bei, den Datenverkehr zu schützen und die Auswirkungen eines kompromittierten Schlüssels oder eines kryptografischen Durchbruchs zu minimieren.

2. Zugangs- bzw. Zugriffs- und Standortkontrollen

(a) Standortkontrollen.

Rechenzentrums-Sicherheitsdienst vor Ort. Die Rechenzentren von Google beschäftigen vor Ort einen Sicherheitsdienst, der rund um die Uhr (24 Stunden am Tag, 7 Tage die Woche) für alle Sicherheitsfunktionen des physischen Rechenzentrums verantwortlich ist. Das Sicherheitspersonal vor Ort kontrolliert Videoüberwachungskameras und alle Alarmsysteme. Das Sicherheitspersonal vor Ort unternimmt regelmäßig Kontrollgänge innerhalb und außerhalb des Rechenzentrums.

Zugangsverfahren in Rechenzentren. Google unterhält formelle Zugangsverfahren für den physischen Zugang zu den Rechenzentren. Die Rechenzentren befinden sich in Einrichtungen, bei denen für den Zugang eine elektronische Schlüsselkarte erforderlich ist, mit Alarmen, die mit dem Sicherheitsdienst vor Ort verbunden sind. Alle Personen, die das Rechenzentrum betreten, müssen sich identifizieren und bei dem Sicherheitsdienst vor Ort ausweisen. Der Zugang zu den Rechenzentren ist nur autorisierten Mitarbeitern, Auftragnehmern und Besuchern gestattet. Nur autorisierte Mitarbeiter und Auftragnehmer dürfen Zugang zu diesen Einrichtungen mit elektronischem Kartenschlüssel anfordern. Anfragen nach elektronischen Schlüsselkarten für den Zugang zu Rechenzentren müssen per E-Mail erfolgen und müssen durch den Manager des Anfragenden und den Direktor des Rechenzentrums genehmigt

werden. Alle anderen eintretenden Personen, die einen temporären Zutritt zu einem Rechenzentrum benötigen, müssen (i) im Voraus die Genehmigung durch den Manager des Rechenzentrums für das konkrete Rechenzentrum und die einzelnen internen Bereiche einholen, die sie besuchen möchten, (ii) sich beim Sicherheitsdienst vor Ort anmelden und (iii) einen bewilligten Antrag auf Zutritt zum Rechenzentrum vorweisen, der für diese Person ausgestellt wurde.

Sicherheitsvorrichtungen vor Ort im Rechenzentrum. Die Rechenzentren von Google verwenden ein doppeltes Authentifizierungs-Zugangskontrollsystem, das mit einem Systemalarm verbunden ist. Das Zugangskontrollsystem überwacht und protokolliert die elektronischen Schlüsselkarten jeder einzelnen Person und wann sie Zugang zu Außentüren, Versand- und Empfangsbereichen und anderen kritischen Bereichen erhalten. Unbefugte Aktivitäten und fehlgeschlagene Zugangsversuche werden vom Zugangskontrollsystem protokolliert und gegebenenfalls untersucht. Der autorisierte Zugang zu den Geschäftsräumen und Rechenzentren ist je nach Zone und Aufgabenbereich der einzelnen Personen beschränkt. Die Brandschutztüren in den Rechenzentren sind mit Alarmanlagen ausgestattet. Sowohl innerhalb als auch außerhalb der Rechenzentren sind CCTV-Kameras in Betrieb. Die Kameras sind so positioniert, dass sie strategische Bereiche abdecken, darunter unter anderem den Außenbereich, die Türen zum Rechenzentrumsgebäude und den Versand-/Empfangsbereich. Das Sicherheitspersonal vor Ort verwaltet die CCTV-Überwachungs-, Aufzeichnungs- und Steuerungsgeräte. Die CCTV-Geräte sind über sichere Kabel im gesamten Rechenzentrum miteinander verbunden. Die Kameras zeichnen vor Ort über digitale Videorekorder 24 Stunden am Tag, 7 Tage die Woche auf. Die Überwachungsaufzeichnungen werden je nach Aktivität bis zu 30 Tage lang aufbewahrt.

(b) Zugriffskontrolle

Infrastruktursicherheitspersonal. Google verfügt über eine Sicherheitsrichtlinie für seine Mitarbeiter, die regelmäßig aktualisiert wird, und verlangt von seinen Mitarbeitern die Teilnahme an Sicherheitsschulungen als Teil des Schulungsprogramms. Das Infrastruktursicherheitspersonal von Google ist für die kontinuierliche Überwachung der Sicherheitsinfrastruktur von Google, die Überprüfung der Dienste und die Reaktion auf Sicherheitsvorfälle verantwortlich.

Zugriffssteuerung und Rechteverwaltung. Administratoren und Endnutzer des Kunden müssen sich über ein zentrales Authentifizierungssystem oder über ein Einmalanmeldungssystem (Single Sign-On, SSO) authentifizieren, um die Dienste nutzen zu können.

Interne Datenzugriffsprozesse und -richtlinien – Access Policy. Die internen Datenzugriffsprozesse und -richtlinien von Google sind so gestaltet, dass sie verhindern, dass unbefugte Personen und/oder Systeme Zugriff auf Systeme erhalten, die zur Verarbeitung von Kundendaten verwendet werden. Google gestaltet seine Systeme so, dass (i) nur autorisierten Personen der Zugriff auf Daten gewährt wird, für die sie zugriffsberechtigt sind, und (ii) sichergestellt ist, dass Kundendaten während der Verarbeitung, während der Nutzung und nach der Aufzeichnung nicht ohne Autorisierung gelesen, kopiert, geändert oder entfernt werden können. Die Systeme sind darauf ausgelegt, unangemessene Zugriffe zu erkennen. Google setzt ein zentralisiertes Zugriffsverwaltungssystem zur Kontrolle von Mitarbeiterzugriffen auf Produktionsserver ein und gewährt nur einem beschränkten Kreis von berechtigten Mitarbeitern Zugriff. Die Authentifizierungs- und Autorisierungssysteme von Google verwenden SSH-Zertifikate sowie Sicherheitsschlüssel und sind so angelegt, dass Google sichere und flexible Zugriffsmechanismen hat. Diese Mechanismen sind so konzipiert, dass nur mit entsprechender

Berechtigung Zugriffe auf Site-Hosts, Logdateien, Daten und Konfigurationsinformationen gewährt werden. Google verlangt die Verwendung eindeutiger Nutzer-IDs, starker Passwörter, der 2-Faktor-Authentifizierung und sorgfältig überwachter Zugriffslisten, um die Möglichkeiten einer unberechtigten Nutzung des Kontos zu minimieren. Die Gewährung oder die Änderung von Zugriffsrechten für berechtigtes Personal basiert auf folgenden Faktoren: dem beruflichen Aufgabenbereich der jeweiligen Person, den notwendigen Anforderungen der jeweiligen Tätigkeit, um berechnete Aufgaben auszuführen, und basierend auf einer zwingenden Erfordernis. Die Gewährung oder Änderung von Zugriffsrechten muss außerdem den internen Datenzugriffsrichtlinien und Schulungen von Google entsprechen. Zugriffsberechtigungen werden über workflowbasierte Werkzeuge verwaltet, die Audit-Datensätze über alle Änderungen erstellen. Der Zugriff auf Systeme wird protokolliert, um einen Audit-Trail zur Rechenschaftspflicht zu erstellen. Wo Passwörter zur Authentifizierung eingesetzt werden (z. B. zum Login an Arbeitsplatzrechnern), sind Passwortrichtlinien eingerichtet worden, die mindestens dem Industriestandard entsprechen. Diese Standards umfassen Einschränkungen bei der Wiederverwendung von Passwörtern und eine ausreichende Passwortstärke. Für den Zugriff auf besonders vertrauliche Informationen (z. B. Kreditkartendaten) verwendet Google Hardwaretokens.

3. Daten

(a) *Datenspeicherung, -isolierung und -Logging.* Google speichert die Daten in einer Multi-Tenant-Umgebung auf Servern, die im Eigentum von Google stehen. Vorbehaltlich anderslautender Weisungen (z. B. in Form der Auswahl eines Speicherorts von Daten) repliziert Google Kundendaten zwischen mehreren geografisch verteilten Rechenzentren. Außerdem isoliert Google die Kundendaten logisch. Der Kunde erhält die Kontrolle über bestimmte Richtlinien für die Datenweitergabe. Diese Richtlinien ermöglichen es dem Kunden in Übereinstimmung mit den Funktionen der Dienste, die für seine Endnutzer geltenden Produktfreigabeeinstellungen für bestimmte Zwecke zu bestimmen. Der Kunde kann die Loggingfunktion nutzen, die Google über die Dienste zur Verfügung stellt.

(b) *Ausgemusterte Festplatten und Richtlinie zur Löschung von Festplatten.* Festplatten, die Daten enthalten, können Leistungsprobleme, Fehler oder Hardwareausfälle aufweisen, die dazu führen, dass sie ausgemustert werden („ausgemusterte Festplatten“). Jede ausgemusterte Festplatte wird einer Reihe von Datenvernichtungsprozessen unterzogen (der „Richtlinie zur Löschung von Festplatten“), bevor sie das Betriebsgelände von Google zur Wiederverwendung oder Vernichtung verlässt. Ausgemusterte Festplatten werden in einem mehrstufigen Prozess gelöscht. Die vollständige Löschung muss daraufhin von mindestens zwei unabhängigen Prüfern bestätigt werden. Die Löschergebnisse werden zur Nachverfolgung anhand der Seriennummer der ausgemusterten Festplatte protokolliert. Schließlich wird die gelöschte außer Betrieb genommene Festplatte für die Wiederverwendung und den erneuten Einsatz freigegeben. Wenn die außer Betrieb genommene Festplatte aufgrund eines Hardwarefehlers nicht gelöscht werden kann, wird sie sicher gelagert, bis sie vernichtet werden kann. Jede Einrichtung wird regelmäßig überprüft, um die Einhaltung der Richtlinie zur Festplattenlöschung zu überwachen.

4. Personalsicherheit

Die Mitarbeiter von Google sind verpflichtet, sich gemäß den Richtlinien des Unternehmens in Bezug auf Vertraulichkeit, Geschäftsethik, angemessene Nutzung und berufliche Standards zu verhalten. Google führt im Rahmen des gesetzlich Zulässigen und in Übereinstimmung mit den geltenden lokalen Arbeitsgesetzen und gesetzlichen Bestimmungen angemessene Hintergrundüberprüfungen durch.

Die Mitarbeiter von Google sind verpflichtet, eine Vertraulichkeitsvereinbarung zu unterzeichnen und den Erhalt sowie die Einhaltung der Vertraulichkeits- und Datenschutzrichtlinien von Google zu bestätigen. Die Mitarbeiter erhalten eine Sicherheitsschulung. Mitarbeiter, die mit Kundendaten umgehen, müssen zusätzliche Anforderungen erfüllen, die ihrer Rolle angemessen sind (z. B. Zertifizierungen). Die Mitarbeiter von Google verarbeiten Kundendaten nicht ohne Genehmigung.

5. Sicherheit von Unterauftragsverarbeitern

Vor der Beauftragung von Unterauftragsverarbeitern führt Google eine Prüfung der Sicherheits- und Datenschutzpraktiken der Unterauftragsverarbeiter durch, um sicherzustellen, dass diese ein Sicherheits- und Datenschutzniveau bieten, das ihrem Zugriff auf Daten und dem Umfang der von ihnen zu erbringenden Dienstleistungen angemessen ist. Nachdem Google die von dem Unterauftragsverarbeiter ausgehenden Risiken bewertet hat, muss der Unterauftragsverarbeiter vorbehaltlich der in Abschnitt 11.3 (Anforderungen an den Einsatz von Unterauftragsverarbeitern) beschriebenen Anforderungen angemessene Vertragsbedingungen in Bezug auf Sicherheit, Vertraulichkeit und Datenschutz vereinbaren.

Anhang 3: Spezifische Datenschutzgesetze

Die Bestimmungen in den einzelnen Unterabschnitten dieses Anhangs 3 gelten nur dort, wo die Verarbeitung personenbezogener Kundendaten dem entsprechenden Gesetz unterliegt.

Europäisches Datenschutzrecht

1. Weitere Definitionen.

- „Land mit angemessenem Datenschutzniveau“ bedeutet:
 - (a) für Daten, die gemäß der EU-DSGVO verarbeitet werden: der Europäische Wirtschaftsraum oder ein Land oder Gebiet, das gemäß der EU-DSGVO einen angemessenen Schutz gewährleistet;
 - (b) für Daten, die gemäß der UK-DSGVO verarbeitet werden: das Vereinigte Königreich oder ein Land oder Gebiet, das gemäß der UK-DSGVO und dem Data Protection Act 2018 einen angemessenen Schutz gewährleistet;
 - (c) für Daten, die gemäß dem Schweizer Datenschutzgesetz verarbeitet werden: die Schweiz oder ein Land oder Gebiet, das
 - (i) in der vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten veröffentlichten Liste der Staaten aufgeführt ist, deren Gesetzgebung einen angemessenen Datenschutz gewährleistet, oder das

(ii) vom Bundesrat der Schweiz und gemäß Schweizer Datenschutzgesetz als Land oder Gebiet anerkannt ist, das einen angemessenen Datenschutz gewährleistet.

In keinem der genannten Fälle darf die Feststellung eines angemessenen Datenschutzniveaus auf einem optionalen Datenschutz-Rahmenwerk basieren.

- „*Alternative Übertragungslösung*“ bezeichnet eine andere Lösung als Standardvertragsklauseln (SCC), die die rechtmäßige Übermittlung personenbezogener Daten in ein Drittland gemäß europäischem Datenschutzrecht ermöglicht, z. B. ein Rahmenwerk zum Datenschutz, das anerkanntermaßen sicherstellt, dass die teilnehmenden Rechtssubjekte einen angemessenen Schutz bieten.
- „*Standardvertragsklauseln für Kunden*“ (Kunden SCC) bezeichnet je nach Anwendbarkeit die Standardvertragsklauseln (Verantwortlicher an Auftragsverarbeiter) die Standardvertragsklauseln (Auftragsverarbeiter an Auftragsverarbeiter) oder die Standardvertragsklauseln (Auftragsverarbeiter an Verantwortlichen).
- „*Standardvertragsklauseln*“ bezeichnet je nach Anwendbarkeit die Standardvertragsklauseln für Kunden oder die Standardvertragsklauseln (Auftragsverarbeiter an Auftragsverarbeiter mit Google als Exporteur).
- „*Standardvertragsklauseln (Verantwortlicher an Auftragsverarbeiter)*“ bezeichnet die Bestimmungen unter <https://cloud.google.com/terms/sccs/eu-c2p>.
- „*Standardvertragsklauseln (Auftragsverarbeiter an Verantwortlichen)*“ bezeichnet die Bestimmungen unter <https://cloud.google.com/terms/sccs/eu-p2c>.
- „*Standardvertragsklauseln (Auftragsverarbeiter an Auftragsverarbeiter)*“ bezeichnet die Bestimmungen unter <https://cloud.google.com/terms/sccs/eu-p2p>.
- „*Standardvertragsklauseln (Auftragsverarbeiter an Auftragsverarbeiter mit Google als Exporteur)*“ bezeichnet die Bestimmungen unter <https://cloud.google.com/terms/sccs/eu-p2p-google-exporter>.

2. Benachrichtigungen über Weisungen. Unbeschadet der Verpflichtungen von Google gemäß Abschnitt 5.2 (Einhaltung der Weisungen des Kunden) oder anderer Rechte oder Pflichten einer der Parteien gemäß der anwendbaren Vereinbarung benachrichtigt Google den Kunden unverzüglich, wenn nach Ansicht von Google:

- a. europäisches Recht Google verbietet, eine Weisung zu befolgen;
- b. eine Weisung gegen europäisches Datenschutzrecht verstößt; oder
- c. Google anderweitig nicht in der Lage ist, eine Weisung zu befolgen.

Dies gilt jeweils, sofern eine solche Benachrichtigung nicht durch europäisches Recht verboten ist.

Wenn der Kunde ein Auftragsverarbeiter ist, leitet er jede Benachrichtigung, die Google gemäß diesem Unterabschnitt zur Verfügung stellt, an den entsprechenden datenschutzrechtlich Verantwortlichen weiter.

3. Auditrechte des Kunden. Google ermöglicht dem Kunden oder einem vom Kunden beauftragten unabhängigen Prüfer die Durchführung von Prüfungen (einschließlich Inspektionen) gemäß Abschnitt 7.5.2(a) (Vom Kunden durchgeführte Audits). Während eines solchen Audits stellt Google alle Informationen zur Verfügung, die erforderlich sind, um nachzuweisen, dass Google seine Verpflichtungen aus diesem Zusatz einhält, und trägt zum Audit bei wie in Abschnitt 7.5 (Überprüfungen und Compliance-Audits) und in diesem Unterabschnitt beschrieben.

4. Datentransfers.

4.1 Eingeschränkte Transfers. Die Parteien erkennen an, dass das europäische Datenschutzrecht keine Standardvertragsklauseln und keine alternative Übertragungslösung erfordert, damit personenbezogene Kundendaten in einem Land mit angemessenem Datenschutzniveau verarbeitet oder dorthin übertragen werden können. Wenn personenbezogene Kundendaten in ein anderes Land übertragen werden und für diese Übermittlungen europäisches Datenschutzrecht gilt (wie vom Kunden gemäß Abschnitt 4.2 „Angabepflicht für Kunden außerhalb von EMEA“ dieser Bestimmungen für europäisches Datenschutzrecht bestätigt, wenn seine Rechnungsadresse außerhalb von EMEA liegt) („Eingeschränkte Transfer“), gilt Folgendes:

a. Wenn Google eine alternative Übertragungslösung für eingeschränkte Transfers zur Verfügung stellt, informiert Google den Kunden über die entsprechende Lösung und stellt sicher, dass eingeschränkte Transfers in Übereinstimmung mit dieser Lösung durchgeführt werden; oder

b. Wenn Google keine alternative Übertragungslösung für eingeschränkte Transfers zur Verfügung stellt oder den Kunden darüber informiert, dass Google eine solche alternative Übertragungslösung nicht mehr anbietet (und auch keinen Ersatz zur Verfügung stellt), gilt Folgendes:

i. Wenn die Adresse von Google in einem Land mit angemessenem Datenschutzniveau ist,

A. gelten die Standardvertragsklauseln (Auftragsverarbeiter an Auftragsverarbeiter mit Google als Exporteur) für alle eingeschränkten Transfers von Google an Unterauftragsverarbeiter; und

B. wenn zusätzlich die Rechnungsadresse des Kunden nicht in einem Land mit angemessenem Datenschutzniveau ist, gelten die Standardvertragsklauseln (Auftragsverarbeiter an Verantwortlichen) – unabhängig davon, ob der Kunde ein Verantwortlicher oder Auftragsverarbeiter ist – in Bezug auf eingeschränkte Transfers zwischen Google und dem Kunden; oder:

ii. wenn sich die Rechnungsadresse von Google nicht in einem Land mit angemessenem Datenschutzniveau befindet, gelten für eingeschränkte Transfers zwischen Google und

dem Kunden die Standardvertragsklauseln (Verantwortlicher an Auftragsverarbeiter) oder die Standardvertragsklauseln (Auftragsverarbeiter an Auftragsverarbeiter) – je nachdem, ob der Kunde Verantwortlicher oder Auftragsverarbeiter ist.

4.2 Angabepflicht für Kunden außerhalb von EMEA. Wenn sich die Rechnungsadresse des Kunden außerhalb von EMEA befindet und die Verarbeitung von personenbezogenen Kundendaten dem europäischen Datenschutzrecht unterliegt, muss der Kunde dies für die anwendbaren Dienste über die Admin-Konsole bestätigen und seine zuständige Aufsichtsbehörde angeben, sofern in Anhang 4 (Bestimmte Produkte) dieses Zusatzes nicht anders angegeben.

4.3 Informationen zu eingeschränkten Transfers. Google stellt dem Kunden folgendermaßen Informationen über eingeschränkte Transfers, zusätzliche Sicherheitskontrollmaßnahmen und andere ergänzende Schutzmaßnahmen zur Verfügung:

- a. wie in Absatz 7.5.1 (Überprüfungen der Sicherheitsdokumentation) beschrieben;
- b. an zusätzlichen Orten wie in Anhang 4 (Bestimmte Produkte) beschrieben; und
- c. Informationen im Zusammenhang mit der Bereitstellung einer alternativen Übertragungslösung unter <https://cloud.google.com/terms/alternative-transfer-solution>.

4.4 SCC-Audits. Wenn Standardvertragsklauseln für den Kunden anwendbar sind, wie in Unterabschnitt 4.1 (Eingeschränkte Transfers) dieser Bestimmungen zum europäischen Datenschutzrecht beschrieben, wird Google dem Kunden oder einem vom Kunden beauftragten unabhängigen Prüfer die Durchführung von Audits gemäß den Standardvertragsklauseln ermöglichen. Während einer Prüfung wird Google alle Informationen zur Verfügung stellen, die durch diese Standardvertragsklauseln angefordert werden. Beides erfolgt in Übereinstimmung mit Abschnitt 7.5.3 (Zusätzliche Geschäftsbedingungen für Überprüfungen und Audits).

4.5 SCC und datenschutzrechtlich verantwortliche Dritte. Ist der Kunde ein Auftragsverarbeiter, erkennt er an, dass Google als weiterer Auftragsverarbeiter möglicherweise nicht in der Lage ist, den datenschutzrechtlich verantwortlichen Dritten zu identifizieren, und leitet daher alle Mitteilungen, die sich auf SCCs beziehen, schnellstmöglich und unverzüglich an den datenschutzrechtlich verantwortlichen Dritten weiter.

4.6 Kündigung aufgrund von Risiken bei Datentransfers. Wenn der Kunde auf der Basis seiner aktuellen oder beabsichtigten Nutzung der Dienste zu dem Schluss kommt, dass keine geeigneten Maßnahmen zum Schutz der transferierten personenbezogenen Kundendaten ergriffen werden, kann der Kunde die Vereinbarung – in Übereinstimmung mit der Regelung zur ordentlichen Kündigung in der Vereinbarung oder, wenn es in der Vereinbarung keine solche Regelung gibt, indem er Google davon in Kenntnis setzt – kündigen.

4.7 Keine Änderung der Standardvertragsklauseln. Nichts in dieser Vereinbarung (einschließlich dieses Zusatzes) hat zum Ziel, Standardvertragsklauseln zu ändern oder ihnen zu widersprechen oder die grundlegenden Rechte oder Freiheiten betroffener Personen gemäß dem europäischen Datenschutzrecht zu beeinträchtigen.

4.8 Vorrang von Standardvertragsklauseln. Bei Widersprüchen oder Unstimmigkeiten zwischen den Standardvertragsklauseln des Kunden (die durch Verweis in diesen Zusatz einbezogen werden) und den übrigen Bestimmungen in der Vereinbarung (einschließlich dieses Zusatzes) sind die Standardvertragsklauseln des Kunden maßgeblich.

5. Anforderungen an den Einsatz von Unterauftragsverarbeitern. Gemäß europäischem Datenschutzrecht ist Google verpflichtet, durch einen schriftlichen Vertrag dafür zu sorgen, dass die in diesem Zusatz beschriebenen Datenschutzpflichten gemäß Art. 28 Abs. 3 DSGVO allen Unterauftragsverarbeitern von Google auferlegt werden.

CCPA

1. Weitere Definitionen.

- „CCPA“ bezeichnet das kalifornische Gesetz zum Schutz der Privatsphäre von Verbrauchern (California Consumer Privacy Act) von 2018 mit jeglichen Ergänzungen, einschließlich des kalifornischen Datenschutzgesetzes (California Privacy Rights Act, CPRA) von 2020 und mit allen Durchführungsbestimmungen.
- „Personenbezogene Kundendaten“ schließt „personenbezogene Daten“ ein.
- Die Begriffe „Unternehmen“, „geschäftlicher Zweck“, „Verbraucher“, „personenbezogene Daten“, „Verarbeitung“, „Verkauf“, „verkaufen“, „Dienstanbieter“ und „weitergeben“ haben die im CCPA angegebenen Bedeutungen.

2. Verbote. Unbeschadet der Verpflichtungen von Google gemäß Abschnitt 5.2 (Einhaltung der Weisungen des Kunden) im Hinblick auf die Verarbeitung personenbezogener Kundendaten gemäß des CCPA wird Google Folgendes unterlassen, falls nicht anderweitig gemäß CCPA dazu befugt:

- a. Personenbezogene Kundendaten verkaufen oder weitergeben;
- b. personenbezogene Kundendaten aufbewahren, verwenden oder offenlegen:
 - i. für andere als für geschäftliche Zwecke gemäß CCPA und im Namen des Kunden oder für die Bereitstellung der Dienste und TSD (soweit anwendbar); oder
 - ii. außerhalb der direkten Geschäftsbeziehung zwischen Google und dem Kunden; oder
- c. um personenbezogene Kundendaten mit personenbezogenen Daten zu kombinieren oder zu aktualisieren, die Google von oder im Auftrag eines Drittanbieters erhält oder bei seinen eigenen Interaktionen mit Verbrauchern erhebt.

3. Compliance. Unbeschadet der Verpflichtungen von Google gemäß Abschnitt 5.2 (Einhaltung der Weisungen des Kunden) oder anderer Rechte oder Pflichten einer der Parteien gemäß der anwendbaren Vereinbarung benachrichtigt Google den Kunden, wenn Google nicht in der Lage ist, seinen Verpflichtungen gemäß CCPA nachzukommen, sofern eine solche Benachrichtigung nicht gesetzlich verboten ist.

4. Intervention des Kunden. Wenn Google den Kunden über die nicht autorisierte Verwendung personenbezogener Kundendaten in Kenntnis setzt, einschließlich unter Abschnitt 3 (Compliance) dieses Absatzes oder Abschnitt 7.2.1 (Meldung eines Vorfalls), kann der Kunde folgende angemessene und geeignete Schritte unternehmen, um diese nicht autorisierte Verwendung zu unterbinden:

- a. von Google empfohlene Maßnahmen gemäß Abschnitt 7.2.2 (Details zu Datenvorfällen), falls zutreffend; oder
- b. Schritte zur Ausübung seiner Rechte gemäß Abschnitt 7.5.2(a) (Vom Kunden durchgeführte Audits) oder 9.1 (Zugriff; Berichtigung; eingeschränkte Verarbeitung; Übertragbarkeit).

Türkei

1. Weitere Definitionen.

- „*Türkisches Datenschutzrecht*“ bezeichnet das am 7. April 2016 in Kraft getretene türkische Gesetz zum Schutz personenbezogener Daten Nr. 6698.
- „*Türkische Datenschutzaufsichtsbehörde*“ bezeichnet die Kişisel Verileri Koruma Kurumu.
- „*Türkische Standardvertragsklauseln*“ bezeichnet die Standardvertragsklauseln gemäß dem türkischen Datenschutzrecht.

2. Datenübertragungen.

2.1 Ergänzende Bedingungen. Wenn sich die Rechnungsadresse des Kunden in der Türkei befindet und Google optionale Zusatzbedingungen (einschließlich der türkischen Standardvertragsklauseln) für die Annahme durch den Kunden in Bezug auf die Übermittlung von personenbezogenen Kundendaten gemäß dem türkischen Datenschutzrecht bereitstellt, ergänzen diese Bestimmungen diesen Zusatz ab dem Datum, an dem sie der türkischen Datenschutzaufsichtsbehörde gemäß Abschnitt 2.2 (Benachrichtigung der zuständigen Behörde) unten wie vom Kunden gegenüber Google nachgewiesen mitgeteilt wurden.

2.2 Benachrichtigung der zuständigen Behörde. Wenn der Kunde gemäß diesem Abschnitt 2 (Datentransfers) türkische Standardvertragsklauseln abschließt, ist der Kunde dafür verantwortlich, die türkische Datenschutzaufsichtsbehörde innerhalb von fünf (5) Arbeitstagen nach Unterzeichnung der türkischen Standardvertragsklauseln über deren Nutzung zu informieren, wie es das türkische Datenschutzrecht verlangt.

2.3 Audits von Standardvertragsklauseln. Wenn der Kunde gemäß diesem Abschnitt 2 (Datentransfers) türkische Standardvertragsklauseln abschließt, gestattet Google dem Kunden oder einem vom Kunden beauftragten unabhängigen Prüfer, Audits wie in diesen Standardvertragsklauseln beschrieben durchzuführen, und stellt während eines Audits alle von diesen Standardvertragsklauseln geforderten Informationen gemäß Abschnitt 7.5.3 (Zusätzliche Geschäftsbedingungen für Überprüfungen und Audits) bereit.

2.4 Kündigung aufgrund von Risiken bei Datentransfers Wenn der Kunde auf der Basis seiner aktuellen oder beabsichtigten Nutzung der Dienste zu dem Schluss kommt, dass keine geeigneten Maßnahmen

zum Schutz der transferierten personenbezogenen Kundendaten ergriffen werden, kann der Kunde die Vereinbarung – in Übereinstimmung mit der Regelung zur ordentlichen Kündigung in der Vereinbarung oder, wenn es in der Vereinbarung keine solche Regelung gibt, indem er Google davon in Kenntnis setzt – kündigen.

2.5 Keine Änderung der türkischen Standardvertragsklauseln. Kein Bestandteil der Vereinbarung (einschließlich dieses Zusatzes) hat zum Ziel, die türkischen Standardvertragsklauseln zu ändern oder ihnen zu widersprechen. Außerdem werden durch diese Vereinbarung nicht die grundlegenden Rechte oder Freiheiten betroffener Personen gemäß dem türkischen Datenschutzrecht beeinträchtigt.

2.6 Vorrang von Standardvertragsklauseln. Bei Widersprüchen oder Unstimmigkeiten zwischen den türkischen Standardvertragsklauseln (die durch Verweis in diesen Zusatz einbezogen werden, wenn sie vom Kunden abgeschlossen wurden) und den übrigen Bestimmungen in der Vereinbarung (einschließlich dieses Zusatzes) sind die türkischen Standardvertragsklauseln maßgeblich.

Israel

1. Zusätzliche Definition.

- „*Israelisches Datenschutzgesetz*“ bezeichnet das israelische Datenschutzgesetz von 1981 und alle darunter erlassenen Vorschriften.

2. Gleichbedeutende Begriffe. Alle mit „Verantwortlicher“, „personenbezogene Daten“, „Verarbeitung“ und „Auftragsverarbeiter“ gleichbedeutenden Begriffe, wie in diesem Zusatz verwendet, haben die im israelischen Datenschutzgesetz angegebenen Bedeutungen.

3. Auditrechte des Kunden. Google ermöglicht dem Kunden oder einem vom Kunden beauftragten unabhängigen Prüfer die Durchführung von Audits (einschließlich Inspektionen) gemäß Abschnitt 7.5.2(a) (Vom Kunden durchgeführte Audits).

Brasilien

1. Zusätzliche Definitionen.

- „*Angemessenes Land*“ bezeichnet für Daten, die gemäß der LGPD verarbeitet werden, Brasilien oder ein Land oder eine internationale Organisation, die von der brasilianischen Datenschutzbehörde (ANPD, portugiesische Abkürzung) als Land anerkannt ist, das einen angemessenen Schutz gemäß der LGPD gewährleistet.
- „*Alternative Übertragungslösung*“ bezeichnet im Sinne dieser brasilianischen Bestimmungen eine Lösung, die nicht den BR-SCCs entspricht und die rechtmäßige internationale Übertragung personenbezogener Daten gemäß der LGPD ermöglicht.
- „*BR SCCs*“ bezeichnet die BR SCCs (Controller-to-Processor), die BR SCCs (Processor-to-Processor) oder die BR SCCs (Processor-to-Processor, Google Exporter), je nach Anwendbarkeit.
- „*BR SCCs (Controller-to-Processor)*“ bezeichnet die Bedingungen unter <https://cloud.google.com/sccs/br-c2p?hl=pt-br>.

- „BR SCCs (Processor-to-Processor)“ bezeichnet die Bedingungen unter <https://cloud.google.com/sccs/br-p2p?hl=pt-br>.
- „BR SCCs (Verarbeiter-zu-Verarbeiter, Google Exporter)“ bezeichnet die Bedingungen unter <https://cloud.google.com/sccs/br-p2p-intra-group?hl=pt-br>.
- „LGPD“ bezeichnet das brasilianische Gesetz Nr. 13.709/2018 in seiner jeweils gültigen Fassung.

2. Benachrichtigungen über Anweisungen. Unbeschadet der Verpflichtungen von Google gemäß Abschnitt 5.2 (Einhaltung der Anweisungen des Kunden) oder anderer Rechte oder Pflichten einer der Parteien gemäß der geltenden Vereinbarung benachrichtigt Google den Kunden unverzüglich, wenn nach Ansicht von Google:

- a. brasilianisches Recht Google daran hindert, einer Anweisung nachzukommen;
- b. eine Anweisung nicht mit der LGPD vereinbar ist oder
- c. Google aus anderen Gründen nicht in der Lage ist, einer Anweisung nachzukommen,

es sei denn, eine solche Benachrichtigung ist nach brasilianischem Recht verboten.

Wenn der Kunde ein Auftragsverarbeiter ist, leitet er alle von Google gemäß diesem Abschnitt übermittelten Benachrichtigungen unverzüglich an den dritten Verantwortlichen weiter.

3. Datentransfers.

3.1. Eingeschränkte Transfers. Die Parteien erkennen an, dass die LGPD keine BR-SCCs oder eine alternative Übertragungslösung erfordert, damit personenbezogene Daten des Kunden in einem angemessenen Land verarbeitet oder dorthin übertragen werden können. Wenn personenbezogene Daten des Kunden in ein anderes Land übertragen werden und die LGPD für die Übertragungen gilt („BR-eingeschränkte Transfers“), dann gilt Folgendes:

- a. hat Google eine alternative Übertragungslösung für eingeschränkte Übertragungen nach BR eingeführt, informiert Google den Kunden über die entsprechende Lösung und stellt sicher, dass solche eingeschränkten Transfers in Übereinstimmung mit dieser Lösung erfolgen; oder
- b. hat Google keine alternative Übertragungslösung für eingeschränkte Übertragungen nach BR eingeführt oder teilt dem Kunden mit, dass Google keine alternative Übertragungslösung für eingeschränkte Transfers i nach BR mehr einführt (ohne eine Ersatzlösung einzuführen):
 - i. Wenn sich die Adresse von Google in einem angemessenen Land befindet, gelten die BR-SCCs (Auftragsverarbeiter-zu-Auftragsverarbeiter, Google-Exporteur) für solche eingeschränkten Transfers i von Google an Unterauftragsverarbeiter; oder
 - ii. wenn sich die Adresse von Google nicht in einem angemessenen Land befindet, gelten die BR-SCCs (Controller-to-Processor) oder BR-SCCs (Processor-to-Processor) (je nachdem, ob der Kunde ein Controller oder ein Verarbeiter ist) für solche eingeschränkten Transfers zwischen Google und dem Kunden.

3.2. *Informationen zu eingeschränkten Transfers.* Google stellt dem Kunden Informationen zu eingeschränkten Transfers gemäß BR, zusätzlichen Sicherheitskontrollmaßnahmen und anderen ergänzenden Schutzmaßnahmen zur Verfügung:

- a. wie in Abschnitt 7.5.1 (Überprüfung der Sicherheitsdokumentation) beschrieben;
- b. an allen weiteren in Anhang 4 (Spezifische Produkte) beschriebenen Orten; und
- c. in Bezug auf die Einführung einer alternativen Übertragungslösung durch Google unter <https://cloud.google.com/terms/alternative-transfer-solution>.

3.3. *SCCs und Drittverantwortliche.* Wenn der Kunde ein Auftragsverarbeiter ist, erkennt der Kunde an, dass Google als weiterer Auftragsverarbeiter möglicherweise nicht in der Lage ist, den Drittverantwortlichen zu identifizieren, und dementsprechend wird der Kunde:

- a. alle Mitteilungen, die sich auf BR-SCCs beziehen, unverzüglich und ohne unnötige Verzögerung an den Drittverantwortlichen weiterleiten;
- b. zwischen Google und dem Kunden allein dafür verantwortlich sein, die Einhaltung der Transparenzpflichten gemäß den BR-SCCs durch den Drittverantwortlichen sicherzustellen; und
- c. auf schriftliche Anfrage von Google unverzüglich die folgenden Informationen über den Drittverantwortlichen bereitstellen: Name, Unternehmensdaten (z. B. Art des Unternehmens, eingetragene Adresse, Steueridentifikationsnummer), Hauptadresse, E-Mail-Adresse, Kontaktstelle für betroffene Personen und alle Angaben, die gemäß den BR-SCCs in Bezug auf den Vertrag des Kunden mit dem Verantwortlichen erforderlich sind.

3.4. *Kündigung aufgrund von Datenübertragungsrisiken.* Wenn der Kunde aufgrund seiner aktuellen oder beabsichtigten Nutzung der Dienste zu dem Schluss kommt, dass für die übermittelten personenbezogenen Daten des Kunden keine angemessenen Schutzmaßnahmen getroffen werden, kann der Kunde die betreffende Vereinbarung gemäß der Kündigungsklausel dieser Vereinbarung oder, falls keine solche Klausel vorhanden ist, durch Benachrichtigung von Google sofort kündigen.

3.5. *Keine Änderung der SCCs.* Keine Bestimmung der Vereinbarung (einschließlich dieses Nachtrags) beabsichtigt, die BR SCCs zu ändern oder ihnen zu widersprechen.

3.6. *Vorrang der SCCs.* Bei Widersprüchen oder Unstimmigkeiten zwischen den BR-SCCs (Verantwortlicher-Auftragsverarbeiter) und den BR-SCCs (Auftragsverarbeiter-Auftragsverarbeiter) (die gegebenenfalls als Anhänge in diesen Nachtrag aufgenommen wurden) und dem Rest der Vereinbarung (einschließlich dieses Nachtrags) haben die geltenden SCCs Vorrang.

Anhang 4: Bestimmte Produkte

Die Bestimmungen in den einzelnen Absätzen dieses Anhangs 4 gelten nur im Hinblick auf die Verarbeitung von Kundendaten durch den entsprechenden Dienst oder die entsprechenden Dienste.

Google Cloud Platform

1. Weitere Definitionen.

- Sofern in der Vereinbarung nicht definiert, bezeichnet „*Konto*“ das Google Cloud Platform-Konto des Kunden.
- Sofern in der Vereinbarung nicht definiert, bezeichnet „*Kundendaten*“ die Daten, die der Kunde oder die Endnutzer Google über das Konto in der Google Cloud Platform zur Verfügung stellen, sowie die Daten, die der Kunde oder die Endnutzer durch die Nutzung der Google Cloud Platform aus diesen Daten ableiten.
- „*Google Cloud Platform*“ bezeichnet die unter <https://cloud.google.com/terms/services> beschriebenen Google Cloud Platform-Dienste, ausgenommen Angebote von Dritten.
- Sofern in der Vereinbarung nicht definiert, bezeichnet „*Angebote von Dritten*“ (a) Dienste, Software, Produkte und andere Angebote von Dritten, die nicht in die Google Cloud Platform oder die Software integriert sind, (b) Angebote, die unter dem Absatz „Nutzungsbedingungen für Drittanbieter“ der dienstspezifischen Nutzungsbedingungen der Vereinbarung aufgeführt sind, und (c) Betriebssysteme von Drittanbietern.

2. Compliance-Zertifizierungen. Die Compliance-Zertifizierungen der geprüften Dienste der Google Cloud Platform umfassen außerdem Zertifikate für ISO 27017 und ISO 27018 sowie eine PCI-DSS-Konformitätsbescheinigung.

3. Standorte von Rechenzentren. Die Standorte der Google Cloud Platform-Rechenzentren sind unter <https://cloud.google.com/about/locations/> aufgeführt.

4. Informationen zu Unterauftragsverarbeitern. Namen, Standorte und Tätigkeitsbereiche aller Google Cloud Platform-Unterauftragsverarbeiter werden unter <https://cloud.google.com/terms/subprocessors> beschrieben.

5. Cloud-Datenschutzteam. Das Datenschutzteam der Google Cloud Platform kann unter <https://support.google.com/cloud/contact/dpo> kontaktiert werden.

6. Informationen zu eingeschränkten Transfers. Zusätzliche Informationen zu eingeschränkten Transfers, zusätzlichen Sicherheitskontrollmaßnahmen und anderen ergänzenden Schutzmaßnahmen finden Sie unter cloud.google.com/privacy/.

7. Dienstspezifische Nutzungsbedingungen.

Bare-Metal-Solution (Google Cloud Platform)

Die Bare-Metal-Solution bietet nicht virtualisierten Zugriff auf die zugrunde liegenden Infrastrukturressourcen und weist aufgrund ihrer Konzeption bestimmte Besonderheiten auf.

1. Änderungsvereinbarungen. Hinsichtlich der Bare-Metal-Solution gelten für diesen Zusatz folgende Änderungen:

- Die Definition von „Third Party Auditor von Google“ wird folgendermaßen ersetzt:
 - „Third Party Auditor von Google“ bezeichnet einen von Google oder von einem Unterauftragsverarbeiter für die Bare-Metal-Solution ernannten, qualifizierten und unabhängigen externen Prüfer, dessen jeweils aktuelle Identität Google dem Kunden auf Anfrage offenlegt.
- Folgende Begriffe werden gelöscht:
 - Aus Abschnitt 7.1.1 (Sicherheitsmaßnahmen von Google): die Wortgruppe „zur Verschlüsselung von Partnerdaten“;
 - Aus Anhang 2 (Sicherheitsmaßnahmen): die Absätze „Server-Betriebssysteme“ und „Aufrechterhaltung des Geschäftsbetriebs“ in Unterabschnitt 1(a);
 - Aus Anhang 2: die Absätze „Externe Angriffsfläche“, „Intrusion Detection“ und „Verschlüsselungstechnologien“ in Unterabschnitt 1(b) und
 - Aus Anhang 2: die folgenden Sätze in Unterabschnitt 3(a):
 - Google speichert die Daten in einer Multi-Tenant-Umgebung auf Servern, die im Eigentum von Google stehen. Vorbehaltlich anderslautender Weisungen (z. B. in Form der Auswahl eines Speicherorts von Daten) repliziert Google Partnerdaten zwischen mehreren geografisch verteilten Rechenzentren.

2. Compliance-Zertifizierungen und SOC-Berichte. Google oder sein Unterauftragsverarbeiter behält für die Bare-Metal-Solution mindestens Folgendes (oder eine gleichwertige oder verbesserte Alternative) bei, um die anhaltende Wirksamkeit der Sicherheitsmaßnahmen zu verifizieren:

- a. ein Zertifikat für ISO 27001 und eine PCI-DSS-Konformitätsbescheinigung (die „Compliance-Zertifizierungen für die Bare-Metal-Solution“); und
- b. SOC 1- und SOC 2-Berichte, die jährlich auf der Grundlage eines mindestens alle 12 Monate durchgeführten Audits aktualisiert werden (die „SOC-Berichte der Bare-Metal-Solution“).

3. Überprüfungen der Sicherheitsdokumentation. Google stellt dem Kunden die Compliance-Zertifizierungen und die SOC-Berichte für die Bare-Metal-Solution zur Überprüfung zur Verfügung, um nachzuweisen, dass Google seinen Verpflichtungen aus diesem Zusatz nachkommt. Ist der Kunde ein Auftragsverarbeiter, ermöglicht Google dem Kunden, den Zugriff auf die SOC-Berichte für den zuständigen Verantwortlichen gemäß Absatz 7.5.3 (Zusätzliche Geschäftsbedingungen für Überprüfungen und Audits) anzufordern.

4. Verpflichtungen des Kunden. Ohne dass dadurch die ausdrücklichen Verpflichtungen von Google im Zusammenhang mit der Bare-Metal-Solution eingeschränkt werden, unternimmt der Kunde angemessene Schritte, um die Sicherheit der Kundendaten und aller anderen Inhalte, die in der Bare-Metal-Solution gespeichert oder verarbeitet werden, aufrechtzuerhalten.

5. Haftungsausschluss. Ungeachtet anderslautender Bestimmungen in der Vereinbarung (einschließlich dieses Zusatzes) ist Google im Zusammenhang mit der Bare-Metal-Solution für Folgendes nicht verantwortlich:

- a. nicht physische Sicherheit, z. B. Zugriffssteuerung, Verschlüsselung, Firewalls, Antivirenprogramme, Bedrohungserkennung und Sicherheitsscans;
- b. Logging und Monitoring;
- c. Wartung und Support für Komponenten, die nicht zur Hardware gehören;
- d. Datensicherung, einschließlich der Konfiguration von Redundanz oder Hochverfügbarkeit; oder
- e. Richtlinien oder Vorgehensweisen zur Aufrechterhaltung des Geschäftsbetriebs und zur Notfallwiederherstellung.

Außer für die physische Sicherheit der Server der Bare-Metal-Solution trägt der Kunde die alleinige Verantwortung für Schutz, Logging und Monitoring, Wartung und Support sowie Sicherung von Betriebssystemen, Kundendaten, Software und Anwendungen, die der Kunde mit der Bare-Metal-Solution verwendet, darin hochlädt oder darin hostet.

Cloud NGFW (Google Cloud Platform)

Die Cloud NGFW-Version mit dem Namen „Cloud NGFW Enterprise“ („CNE“) soll Cybersecurity-Risiken verringern und hat daher bestimmte spezifische Eigenschaften.

1. Änderungsvereinbarungen. Hinsichtlich CNE gelten für diesen Zusatz folgende Änderungen:

- Die Abschnitte 6.1 (Löschung durch den Kunden) und 6.2 (Rückgabe oder Löschung am Ende der Laufzeit) hindern Google und seine Unterauftragsverarbeiter nicht daran, Dateien oder Netzwerktraffic-Paketaufzeichnungen aufzubewahren, die zu TSD-Zwecken eingereicht und von CNE als Sicherheitsbedrohung eingestuft wurden, sofern die Datei oder Netzwerktraffic-Paketaufzeichnung keine personenbezogenen Kundendaten enthält.

Google Distributed Cloud Connected (Google Cloud Platform)

Google Distributed Cloud Connected wird nicht in einem Google-Rechenzentrum bereitgestellt und hat designbedingt bestimmte spezifische Eigenschaften.

1. Änderungsvereinbarungen. Hinsichtlich Google Distributed Cloud Connected gelten für diesen Zusatz folgende Änderungen:

- Verweise auf „die Systeme von Google“ werden durch „die Geräte“ ersetzt.

- Absatz 6.2 (Rückgabe oder Löschung am Ende der Laufzeit) wird folgendermaßen ersetzt:
 - *6.2 Rückgabe oder Löschung am Ende der Laufzeit.* Der Kunde weist Google an, zum Ende der Laufzeit alle Kundendaten (einschließlich vorhandener Kopien) gemäß anwendbarem Recht aus den Systemen zu löschen. Wenn der Kunde Kundendaten nach dem Ende der Laufzeit behalten möchte, kann er diese Daten vor Ende der Laufzeit exportieren oder kopieren. Google wird der Weisung in diesem Abschnitt 6.2 Folge leisten, sobald dies vernünftigerweise möglich ist, spätestens aber innerhalb einer Höchstfrist von 180 Tagen, sofern nicht europäisches Recht, wo europäisches Datenschutzrecht gilt, oder anderes Recht, wo andere Datenschutzgesetze Anwendung finden, eine Aufbewahrung vorschreibt.
- Am Ende von Abschnitt 10.1 (Einrichtungen zur Datenspeicherung und -verarbeitung) werden folgende Wörter hinzugefügt: „oder wo der Kunde seinen Standort hat.“
- Absatz 1 (Rechenzentrums- und Netzwerksicherheit) von Anhang 2 (Sicherheitsmaßnahmen) wird folgendermaßen ersetzt:
 - **1. Sicherheit lokaler Computer und Netzwerksicherheit**

Lokale Computer. Kundendaten werden ausschließlich auf den Geräten gespeichert, die an einem Kundenstandort bereitgestellt werden sollen.

Server-Betriebssysteme. Google-Server verwenden eine Linux-basierte Implementierung, die an die Anwendungsumgebung angepasst ist. Google verwendet einen Prozess zur Codeüberprüfung, um die Sicherheit des Codes für die Bereitstellung von Google Distributed Cloud Connected zu erhöhen und die Sicherheitsprodukte in Produktionsumgebungen von Google Distributed Cloud Connected zu verbessern.

Verschlüsselungstechnologien. Google stellt eine HTTPS-Verschlüsselung (auch SSL- oder TLS-Verbindung genannt) zur Verfügung und ermöglicht die Verschlüsselung von Daten während der Übertragung. Google-Server unterstützen einen Austausch von RSA- und ECDSA-signierten Schlüsseln nach Diffie-Hellman auf Basis sitzungsspezifischer Elliptische-Kurven-Kryptografie. Diese PFS-Methoden (Perfect Forward Secrecy) tragen dazu bei, den Datenverkehr zu schützen und die Auswirkungen eines kompromittierten Schlüssels oder eines kryptografischen Durchbruchs zu minimieren. Google stellt auch die Verschlüsselung von ruhenden Daten mit mindestens AES128 oder einer vergleichbaren Lösung zur Verfügung. Google Distributed Cloud Connected verfügt über eine CMEK-Integration. Weitere Informationen finden Sie unter <https://cloud.google.com/kms/docs/cmek>.

Verbindung zu Cloud VPN. Google ermöglicht dem Kunden, eine starke, verschlüsselte Verbindung zwischen den Geräten und der Virtual Private Cloud des Kunden zu aktivieren und zu konfigurieren, indem er Cloud VPN über eine IPSEC-VPN-Verbindung verwendet.

Gebundener Speicher. Der Datenspeicher des Kunden ist an den Server gebunden. Sollte ein Datenträger im ruhenden Zustand gestohlen oder kopiert werden, ist der darauf gespeicherte Inhalt außerhalb des Servers nicht wiederherstellbar.

- Die Absätze 2 (Zugriffs- und Zutrittskontrollen) und 3 (Daten) von Anhang 2 (Sicherheitsmaßnahmen) werden gelöscht.

2. Nicht anwendbare Regelungen. Jedwede Verpflichtungen von Google in der Vereinbarung (einschließlich dieses Zusatzes) oder Aussagen in zugehöriger Sicherheitsdokumentation (einschließlich Whitepapers), die vom Betrieb eines Google-Rechenzentrums durch Google abhängen, gelten nicht für Google Distributed Cloud Connected.

Google-Managed Multi-Cloud (Google Cloud Platform)

Google-Managed Multi-Cloud Services umfassen Infrastruktur von Drittanbietern und haben designbedingt bestimmte spezifische Eigenschaften.

1. Zusätzliche Definition.

- „Zusatz zur Datenverarbeitung für Google-Managed Multi-Cloud Services“ bezeichnet die Bestimmungen unter <https://cloud.google.com/terms/mcs-data-processing-terms>.

2. Datenverarbeitungsbedingungen für die Multi-Cloud. Die Ergänzungsvereinbarung zur Datenverarbeitung für Google-Managed Multi-Cloud Services ersetzt und ändert diesen Zusatz im Hinblick auf von Google verwaltete Multi-Cloud Services für die Google Cloud Platform.

Google Cloud VMware Engine (Google Cloud Platform)

Google hat möglicherweise keinen Zugang zur VMware-Umgebung des Kunden und kann möglicherweise personenbezogene Daten in der VMware-Umgebung des Kunden nicht verschlüsseln.

NetApp Volumes (Google Cloud Platform)

1. Änderungsvereinbarungen. Hinsichtlich NetApp Volumes gelten für diesen Zusatz folgende Änderungen:

- Die Definition von „Third-Party Auditor von Google“ wird folgendermaßen ersetzt:
 - *“Third-Party Auditor von Google“* bezeichnet einen von Google oder von einem Unterauftragsverarbeiter für die NetApp Volumes ernannten, qualifizierten und unabhängigen externen Prüfer, dessen jeweils aktuelle Identität Google dem Kunden auf Anfrage offenlegt.
- Absatz 3(a) (Datenspeicherung, -isolierung und -Logging) von Anhang 2 (Sicherheitsmaßnahmen) wird folgendermaßen ersetzt:
 - (a) *Datenspeicherung, -isolierung und -Logging.* Google speichert Daten in einer mandantenfähigen Umgebung auf Servern von NetApp, Inc. Vorbehaltlich anderslautender Weisungen (z. B. in Form der Auswahl eines Speicherorts von Daten) repliziert Google Kundendaten zwischen mehreren geografisch verteilten Rechenzentren. Außerdem isoliert Google die Kundendaten logisch. Der Kunde erhält die Kontrolle über bestimmte Richtlinien für die Datenweitergabe. Diese Richtlinien

ermöglichen es dem Kunden in Übereinstimmung mit der Funktionalität der Dienste, die für seine Endnutzer geltenden Produktfreigabeeinstellungen für bestimmte Zwecke zu bestimmen. Der Kunde kann die Loggingfunktion nutzen, die Google über die Dienste zur Verfügung stellt.

2. Compliance-Zertifizierungen und SOC-Berichte. Google oder sein Unterauftragsverarbeiter erhält für die NetApp Volumes mindestens Folgendes (oder eine gleichwertige oder verbesserte Alternative):

- a. ein Zertifikat für ISO 27001 und eine PCI-DSS-Konformitätsbescheinigung (die „*Compliance-Zertifizierungen für NetApp*“); und
- b. SOC 1- und SOC 2-Berichte, die jährlich auf der Grundlage eines mindestens alle 12 Monate durchgeführten Audits aktualisiert werden (die „*NetApp-SOC-Berichte*“).

3. Überprüfungen der Sicherheitsdokumentation. Google stellt dem Kunden die Compliance-Zertifizierungen für NetApp und die NetApp-SOC-Berichte zu Prüfzwecken zur Verfügung, um damit nachzuweisen, dass Google seinen Verpflichtungen aus dem vorliegenden Zusatz nachkommt. Ist der Kunde Auftragsverarbeiter, ermöglicht Google dem Kunden, den Zugriff auf die NetApp-SOC-Berichte für den datenschutzrechtlich verantwortlichen Dritten gemäß Abschnitt 7.5.3 (Zusätzliche Geschäftsbedingungen für Überprüfungen und Audits) anzufordern.

Google Workspace und Cloud Identity

1. Weitere Definitionen.

- Sofern in der Vereinbarung nicht definiert, bezeichnet „*Konto*“ das Google Workspace- oder Cloud Identity-Konto des Kunden.
- Wenn „*Cloud Identity*“ im Rahmen einer separaten Vereinbarung als eigenständiges Produkt und nicht als Teil der Google Cloud Platform oder von Google Workspace erworben wurde, bezeichnet dieser Produktname die unter <https://cloud.google.com/terms/identity/user-features> beschriebenen Cloud Identity-Dienste.
- Sofern in der Vereinbarung nicht definiert, bezeichnet „*Kundendaten*“ die Daten, die vom Kunden oder dessen Endnutzern oder im Namen des Kunden oder von dessen Endnutzern über das Konto in Google Workspace oder Cloud Identity hochgeladen, gespeichert, gesendet oder empfangen werden.
- „*Google Workspace*“ bezeichnet, soweit anwendbar, die Google Workspace- oder Google Workspace for Education-Dienste, die unter https://workspace.google.com/terms/user_features.html beschrieben sind.

2. Zusätzliche Produkte. Wenn Google dem Kunden nach eigenem Ermessen zusätzliche Produkte für die Verwendung mit Google Workspace oder Cloud Identity gemäß den anwendbaren Nutzungsbedingungen für zusätzliche Produkte zur Verfügung stellt:

- a. kann der Kunde zusätzliche Produkte über die Admin-Konsole aktivieren oder deaktivieren und muss keine zusätzlichen Produkte verwenden, um Google Workspace oder Cloud Identity nutzen zu können; und
- b. wenn der Kunde sich entscheidet, zusätzliche Produkte zu installieren oder mit Google Workspace oder Cloud Identity zu verwenden, können die zusätzlichen Produkte auf Kundendaten zugreifen, soweit dies je nach Anwendungsfall für die Interoperabilität mit Google Workspace oder Cloud Identity erforderlich ist.

Zur Klarstellung: Dieser Zusatz gilt nicht für die Verarbeitung personenbezogener Daten im Zusammenhang mit der Bereitstellung von zusätzlichen Produkten, die vom Kunden installiert oder verwendet werden, einschließlich personenbezogener Daten, die an solche oder von solchen zusätzlichen Produkten übertragen werden.

3. Compliance-Zertifizierungen. Die Compliance-Zertifizierungen der geprüften Dienste von Google Workspace und Cloud Identity umfassen außerdem Zertifikate für ISO 27017 und ISO 27018.

4. Standorte von Rechenzentren. Die Standorte der Rechenzentren von Google Workspace und Cloud Identity sind unter <https://www.google.com/about/datacenters/locations/> aufgeführt.

5. Informationen zu Unterauftragsverarbeitern. Namen, Standorte und Tätigkeitsbereiche der Unterauftragsverarbeiter für Google Workspace und Cloud Identity sind unter <https://workspace.google.com/intl/en/terms/subprocessors.html> beschrieben.

6. Cloud-Datenschutzteam. Das Datenschutzteam für Google Workspace und Cloud Identity kann von Administratoren, die in ihrem Admin-Konto angemeldet sind, unter https://support.google.com/a/contact/googlecloud_dpr kontaktiert werden.

7. Zusätzliche Sicherheitsmaßnahmen. Für Google Workspace und Cloud Identity

- a. Google trennt die Daten eines Endnutzers logisch von den Daten der jeweils anderen Endnutzer; und
- b. Daten für einen authentifizierten Endnutzer werden keinem anderen Endnutzer angezeigt (es sei denn, der authentifizierte Endnutzer oder ein Administrator erlaubt, dass die Daten geteilt werden).

8. Informationen zu eingeschränkten Transfers. Zusätzliche Informationen zu eingeschränkten Transfers, zusätzlichen Sicherheitskontrollmaßnahmen und anderen ergänzenden Schutzmaßnahmen finden Sie unter cloud.google.com/privacy/.

9. Zusatz zu Dienstdaten. Wenn Google im Zusammenhang mit dem vorliegenden Zusatz dem Kunden einen optionalen Zusatz zu Dienstdaten zur Verfügung stellt, stellt die Verfügbarkeit dieses optionalen Zusatzes eine „Aktualisierung des Zusatzes zur Datenverarbeitung“ dar, wenn solch ein Begriff in einem Zusatz zu Dienstdaten definiert ist, der zuvor vom Kunden angenommen wurde.

10. Dienstspezifische Nutzungsbedingungen.

AppSheet (Google Workspace)

1. Änderungsvereinbarungen.

Hinsichtlich AppSheet gelten für diesen Zusatz folgende Änderungen:

- Der Absatz „Server-Betriebssysteme“ unter Unterabschnitt 1(a) des Anhangs 2 (Sicherheitsmaßnahmen) wird wie folgt ersetzt:
 - *Server-Betriebssysteme.* Google-Server verwenden eine Linux-basierte Implementierung, die an die Anwendungsumgebung angepasst ist.

2. Weitere Standorte von Rechenzentren.

Zusätzliche Rechenzentrumsstandorte für AppSheet sind unter <https://cloud.google.com/about/locations/> aufgeführt.

Looker (Original)

1. Weitere Definitionen.

- „Admin-Konsole“ bezeichnet die anwendbaren Admin-Konsolen für die einzelnen Instanzen.
- „Zusatz zur Datenverarbeitung für Google-Managed Multi-Cloud Services“ bezeichnet, soweit anwendbar, die Bestimmungen unter <https://cloud.google.com/terms/mcs-data-processing-terms>.
- „Google-Managed Multi-Cloud Services“ bezeichnet, soweit anwendbar, angegebene Google-Dienste, -Produkte und -Funktionen, die auf der Infrastruktur eines externen Cloud-Anbieters gehostet werden.
- „Looker (Original)“ bezeichnet eine integrierte Plattform (je nach Anwendungsfall einschließlich cloudbasierter Infrastruktur und Softwarekomponenten einschließlich der zugehörigen APIs), die es Unternehmen ermöglicht, Daten zu analysieren und geschäftliche Messwerte über mehrere Datenquellen hinweg zu definieren, die dem Kunden von Google gemäß der Vereinbarung bereitgestellt wurden. Looker (Original) schließt Angebote von Dritten aus.
- „Drittanbieter von Multi-Cloud Services“ hat die in der Ergänzungsvereinbarung zur Datenverarbeitung für Google-Managed Multi-Cloud Services angegebene Bedeutung.
- „Bestellformular“ hat die in der Vereinbarung angegebene Bedeutung, es sei denn, der Kunde hat das Produkt über einen Reseller oder einen Onlinemarktplatz gekauft oder nutzt Looker nur zu Test- oder Evaluierungszwecken gemäß einer Test- oder Evaluierungsvereinbarung. In diesem Fall kann „Bestellformular“ eine andere schriftliche Form (E-Mail oder eine andere zulässige elektronische Form) bezeichnen, die jeweils von Google autorisiert wurde.

2. Änderungsvereinbarungen.

Hinsichtlich Looker (Original) gelten für diesen Zusatz folgende Änderungen:

- Die Definition von „Benachrichtigungs-E-Mail-Adresse“ wird wie folgt ersetzt:
 - „Benachrichtigungs-E-Mail-Adresse“ bezeichnet die vom Kunden im Bestellformular oder über Looker angegebene(n) E-Mail-Adresse(n), die dazu dient bzw. dienen, bestimmte Benachrichtigungen von Google zu erhalten.

- Die Definitionen von „Standardvertragsklauseln (Verantwortlicher an Auftragsverarbeiter)“, „Standardvertragsklauseln (Auftragsverarbeiter an Verantwortlichen)“, „Standardvertragsklauseln (Auftragsverarbeiter an Auftragsverarbeiter)“ und „Standardvertragsklauseln (Auftragsverarbeiter an Auftragsverarbeiter, Google-Exporteur)“ in Anhang 3 (Konkrete Datenschutzgesetze) werden folgendermaßen ersetzt:
 - „Standardvertragsklauseln (Verantwortlicher an Auftragsverarbeiter)“ bezeichnet die Bestimmungen unter <https://cloud.google.com/terms/sccs/eu-c2p>;
 - „Standardvertragsklauseln (Auftragsverarbeiter an Verantwortlichen)“ bezeichnet die Bestimmungen unter <https://cloud.google.com/terms/sccs/eu-p2c>;
 - „Standardvertragsklauseln (Auftragsverarbeiter an Auftragsverarbeiter)“ bezeichnet die Bestimmungen unter <https://cloud.google.com/terms/sccs/eu-p2p> und
 - „Standardvertragsklauseln (Auftragsverarbeiter an Auftragsverarbeiter, Google-Exporteur)“ bezeichnet die Bestimmungen unter <https://cloud.google.com/terms/looker/legal/sccs/eu-p2p-intra-group>.
- Am Ende von Abschnitt 10.1 (Einrichtungen zur Datenspeicherung und -verarbeitung) werden folgende Wörter hinzugefügt: „oder wo Drittanbieter von Multi-Cloud Services Einrichtungen unterhalten.“

3. Zusätzliche Sicherheitsverantwortung des Kunden. Der Kunde ist verantwortlich für die Sicherheit der Umgebung und der Datenbanken des Kunden sowie der Konfiguration von Looker (Original). Davon ausgenommen sind Systeme, die von Google verwaltet und kontrolliert werden.

4. Compliance-Zertifizierungen und SOC-Berichte. Die Compliance-Zertifizierungen und SOC-Berichte für geprüfte Dienste von Looker (Original) können abhängig von der Hostingumgebung, in der die entsprechenden Dienste verwendet werden, variieren. Google stellt auf Anfrage Details zu den Compliance-Zertifizierungen und SOC-Berichten für bestimmte Hostingumgebungen zur Verfügung.

5. Standorte von Rechenzentren. Die Standorte der Rechenzentren von Looker (Original) werden auf dem entsprechenden Bestellformular aufgeführt oder anderweitig von Google ausgewiesen.

6. Keine Angabepflicht für Kunden außerhalb von EMEA. Der Kunde ist nicht zur Angabe oder zur Identifizierung seiner zuständigen Aufsichtsbehörde verpflichtet, wie in Unterabschnitt 4.2 (Angabepflicht für Kunden außerhalb von EMEA) der Bestimmungen unter „Europäisches Datenschutzrecht“ in Anhang 3 (Konkrete Datenschutzgesetze) für Looker (Original) beschrieben.

7. Informationen zu eingeschränkten Transfers. Zusätzliche Informationen zu eingeschränkten Transfers, zusätzlichen Sicherheitskontrollmaßnahmen und anderen ergänzenden Schutzmaßnahmen für Looker (Original) finden Sie unter <https://docs.looker.com>.

8. Informationen zu Unterauftragsverarbeitern. Namen, Standorte und Tätigkeitsbereiche der Unterauftragsverarbeiter für Looker (Original) werden beschrieben unter:

- a. <https://cloud.google.com/terms/looker/privacy/lookeroriginal-subprocessors> und
- b. <https://cloud.google.com/terms/subprocessors>.

9. Google-Managed Multi-Cloud (Looker [Original])

Google-Managed Multi-Cloud Services umfassen Infrastruktur von Drittanbietern und haben designbedingt bestimmte spezifische Eigenschaften.

9.1 *Datenverarbeitungsbedingungen für die Multi-Cloud.* Die Ergänzungsvereinbarung zur Datenverarbeitung für Google-Managed Multi-Cloud Services ersetzt und ändert den vorliegenden Zusatz im Hinblick auf von Google verwaltete Multi-Cloud-Dienste für Looker (Original).

10. Cloud-Datenschutzteam. Das Datenschutzteam für Looker (Original) kann unter <https://support.google.com/cloud/contact/dpo> kontaktiert werden.

11. Verzeichnis von Verarbeitungstätigkeiten von Google. Soweit Google nach anwendbarem Datenschutzrecht verpflichtet ist, Datensätze mit bestimmten Kundeninformationen zu erheben und zu pflegen, stellt der Kunde Google auf Anfrage diese Informationen zur Verfügung und informiert Google über alle erforderlichen Aktualisierungen, um die Informationen korrekt und auf dem neuesten Stand zu halten, es sei denn, Google fordert den Kunden auf, solche Informationen über andere Methoden zur Verfügung zu stellen und zu aktualisieren.

12. Zusätzliche Sicherheitsmaßnahmen für Anwendungen. Google implementiert und verwaltet die unten beschriebenen zusätzlichen Sicherheitsmaßnahmen für Looker (Original):

- a. Die Sicherheitsarchitektur von Google entspricht mindestens dem Branchenstandard. Die für die Anwendungen von Google verwendeten Proxyserver tragen zu einem sicheren Zugriff auf Looker bei. Sie ermöglichen die Filterung von Angriffen durch IP-Sperrlisten und die Beschränkung der Verbindungsrate an einem Punkt.
- b. Die Administratoren des Kunden steuern den Zugriff auf Anwendungen durch Mitarbeiter von Google, die auf Anfrage des Kunden oder der Endnutzer technischen Support bereitstellen.

SecOps-Dienste

1. Weitere Definitionen.

- Sofern in der Vereinbarung nicht definiert, bezeichnet „Konto“ je nach Anwendungsfall das SecOps-Dienste-Konto oder das Google Cloud Platform-Konto des Kunden.
- Sofern in der Vereinbarung nicht definiert, bezeichnet „Kundendaten“ die Daten, die Google vom Kunden oder von den Endnutzern über das SecOps-Dienste-Konto oder für Mandiant Consulting Services und Managed Services im Zusammenhang mit dem Erhalt der Dienste zur Verfügung gestellt werden.
- „Kundenbeauftragter Anbieter“ bezeichnet einen Dienstanbieter (einschließlich eines Auftragsverarbeiters oder Unterauftragsverarbeiters), der vom Kunden im Rahmen einer separaten Vereinbarung zwischen dem Kunden und diesem Anbieter direkt beauftragt wird.

- „SecOps-Dienste“ bezeichnet die unter <https://cloud.google.com/terms/secops/services> beschriebenen SecOps-Dienste. Davon ausgenommen sind Angebote Dritter.
- Sofern in der Vereinbarung nicht definiert, bezeichnet „Angebote von Dritten“ (a) Dienste, Software, Produkte und andere Angebote von Dritten, die nicht in SecOps-Dienste oder -Software integriert sind, und (b) Betriebssysteme von Drittanbietern.

2. Änderungsvereinbarungen. Hinsichtlich SecOps-Diensten gelten für diesen Zusatz folgende Änderungen:

- Die Definition von „Zusätzliche Sicherheitskontrollmaßnahmen“ wird wie folgt ersetzt:
 - „Zusätzliche Sicherheitskontrollmaßnahmen“ bezeichnet Sicherheitsressourcen, Features, Funktionen und/oder Kontrollen (falls vorhanden), die der Kunde nach eigenem Ermessen verwenden kann, einschließlich (falls vorhanden) Verschlüsselung, Logging und Monitoring, Identitäts- und Zugriffsverwaltung und Sicherheitsscans.
- Die Definition für „geprüfte Dienste“ wird wie folgt ersetzt:
 - „Geprüfte Dienste“ bezeichnet die jeweils aktuellen SecOps-Dienste, die unter <https://cloud.google.com/security/compliance/secops/services-in-scope> als in den Geltungsbereich der jeweiligen Zertifizierung oder des Berichts fallend aufgeführt sind. Google darf SecOps-Dienste nicht aus dieser Liste (URL) entfernen, sofern sie nicht in Übereinstimmung mit der anwendbaren Vereinbarung eingestellt wurden.
- Die Definitionen von „Standardvertragsklauseln (Verantwortlicher an Auftragsverarbeiter)“, „Standardvertragsklauseln (Auftragsverarbeiter an Verantwortlichen)“, „Standardvertragsklauseln (Auftragsverarbeiter an Auftragsverarbeiter)“ und „Standardvertragsklauseln (Auftragsverarbeiter an Auftragsverarbeiter, Google-Exporteur)“ in Anhang 3 (Konkrete Datenschutzgesetze) werden folgendermaßen ersetzt:
 - „Standardvertragsklauseln (Verantwortlicher an Auftragsverarbeiter)“ bezeichnet die Bestimmungen unter <https://cloud.google.com/terms/secops/scs/eu-c2p>;
 - „Standardvertragsklauseln (Auftragsverarbeiter an Verantwortlichen)“ bezeichnet die Bestimmungen unter <https://cloud.google.com/terms/secops/scs/eu-p2c>;
 - „Standardvertragsklauseln (Auftragsverarbeiter an Auftragsverarbeiter)“ bezeichnet die Bestimmungen unter <https://cloud.google.com/terms/secops/scs/eu-p2p>; und
 - „Standardvertragsklauseln (Auftragsverarbeiter an Auftragsverarbeiter, Google-Exporteur)“ bezeichnet die Bestimmungen unter <https://cloud.google.com/terms/secops/scs/eu-p2p-google-exporter>.
- Absatz 6.1 (Löschung durch den Kunden) wird folgendermaßen geändert:

- **6.1 Löschung durch den Kunden.** Google ermöglicht dem Kunden, Kundendaten während der Laufzeit in Übereinstimmung mit der Funktionalität der Dienste auf Anfrage zu löschen. Wenn der Kunde die Dienste nutzt, um Kundendaten während der geltenden Laufzeit zu löschen und diese Kundendaten vom Kunden nicht wiederhergestellt werden können, oder wenn der Kunde während der Laufzeit die Löschung von Kundendaten verlangt, begründet diese Verwendung oder Anfrage (soweit anwendbar) eine Anweisung an Google, die relevanten Kundendaten gemäß geltendem Recht aus den Google-Systemen zu löschen. Google wird dieser Weisung Folge leisten, sobald dies vernünftigerweise möglich ist, spätestens aber innerhalb einer Höchstfrist von 180 Tagen, sofern nicht europäisches Recht, wo europäisches Datenschutzrecht gilt, oder anderes Recht, wo andere Datenschutzgesetze Anwendung finden, eine Aufbewahrung vorschreibt.
- Absatz 7.4 (Compliance-Zertifizierungen und SOC-Berichte) des Zusatzes wird folgendermaßen geändert:
 - *7.4 Compliancezertifizierungen und SOC-Berichte.* Google behält für die geprüften Dienste mindestens die unter <https://cloud.google.com/security/compliance/secops/services-in-scope> ausgewiesenen Zertifizierungen und Berichte bei, um die anhaltende Wirksamkeit der Sicherheitsmaßnahmen zu bewerten (die „**Compliance-Zertifizierungen**“ und „**SOC-Berichte**“).

Google kann jederzeit Standards hinzufügen. Google kann eine Compliance-Zertifizierung oder einen SOC-Bericht durch eine gleichwertige oder verbesserte Alternative ersetzen.

- Absatz 9.1 (Zugriff; Berichtigung; Eingeschränkte Verarbeitung; Übertragbarkeit) wird folgendermaßen geändert:

9.1 Zugriff; Berichtigung; eingeschränkte Verarbeitung; Übertragbarkeit. Während der Laufzeit ermöglicht Google dem Kunden in Übereinstimmung mit der Funktionalität der Dienste den Zugriff auf sowie die Berichtigung und die Einschränkung der Verarbeitung von Kundendaten, u. a. wie in Absatz 6.1 (Löschung durch den Kunden) beschrieben, sowie auf Anfrage den Export der Kundendaten. Wenn der Kunde feststellt, dass personenbezogene Kundendaten falsch oder nicht mehr aktuell sind, ist er dafür verantwortlich, Google zu benachrichtigen, und Google wird den Kunden bei der Berichtigung dieser Daten unterstützen, sofern dies nach dem anwendbaren Datenschutzrecht erforderlich ist.

3. Standorte von Rechenzentren. Die Standorte der Rechenzentren von SecOps-Diensten sind unter <https://cloud.google.com/terms/secops/data-residency> aufgeführt.

4. Keine Angabepflicht für Kunden außerhalb von EMEA. Der Kunde ist nicht zur Angabe oder zur Identifizierung seiner zuständigen Aufsichtsbehörde verpflichtet, wie in Absatz 4.2 (Angabepflicht für Kunden außerhalb von EMEA) der Bestimmungen unter „Europäisches Datenschutzrecht“ in Anhang 3 (Konkrete Datenschutzgesetze) für SecOps-Dienste beschrieben.

5. Informationen zu Unterauftragsverarbeitern. Namen, Standorte und Tätigkeitsbereiche der Unterauftragsverarbeiter für SecOps-Dienste sind unter <https://cloud.google.com/terms/secops/subprocessors> beschrieben.

6. Cloud-Datenschutzteam. Das Datenschutzteam für SecOps-Dienste kann unter <https://support.google.com/cloud/contact/dpo> (und/oder über andere von Google gelegentlich zur Verfügung gestellte Methoden) kontaktiert werden.

7. Verzeichnis von Verarbeitungstätigkeiten von Google. Soweit Google nach anwendbarem Datenschutzrecht verpflichtet ist, Datensätze mit bestimmten Kundeninformationen zu erheben und zu pflegen, stellt der Kunde Google auf Anfrage diese Informationen zur Verfügung und informiert Google über alle erforderlichen Aktualisierungen, um die Informationen korrekt und auf dem neuesten Stand zu halten, es sei denn, Google fordert den Kunden auf, solche Informationen über andere Methoden zur Verfügung zu stellen und zu aktualisieren.

8. Dienstspezifische Nutzungsbedingungen.

Mandiant Consulting Services und verwaltete Dienste

Mandiant Consulting Services und verwaltete Dienste stellen Beratungs- und Implementierungsdienste (einschließlich Incident Response, strategischer Bereitschaft und technischer Absicherung zur Abwehr von Bedrohungen und zur Verringerung vorfallbezogener Risiken) und verwaltete Erkennungs- und Reaktionsdienste bereit und haben designbedingt bestimmte spezifische Eigenschaften.

1. Änderungsvereinbarungen. Ausschließlich hinsichtlich Mandiant Consulting Services und verwalteter Dienste gelten für diesen Zusatz folgende Änderungen:

- Die Definition von „Datenvorfall“ wird folgendermaßen ergänzt:
 - Zur Klarstellung: Datenvorfälle umfassen, sofern anwendbar, keine Vorfälle, die Gegenstand der Mandiant Consulting Services und/oder verwalteten Dienste sind.
- Absatz 5.2(b)(i) (Einhaltung der Weisungen des Kunden) wird folgendermaßen ersetzt:
 - i. Nutzung der Dienste durch den Kunden, und
- Der zweite Satz von Absatz 7.1.1 (Sicherheitsmaßnahmen von Google) wird folgendermaßen geändert:
 - Die Sicherheitsmaßnahmen können (je nach Angemessenheit) Maßnahmen zur Verschlüsselung von Kundendaten umfassen; um die kontinuierliche Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste von Google zu gewährleisten; um nach einem Vorfall den zeitnahen Zugriff auf Kundendaten wiederherzustellen; und zur regelmäßigen Wirksamkeitsprüfung.
- Absatz 7.3.1(b) wird folgendermaßen geändert:

- b. die Verwaltung, Zugriffsverwaltung und Sicherung der Kontoauthentifizierungsdaten, Systeme, Software, Netzwerke und Geräte, die der Kunde verwendet, um die Mandiant Consulting Services und/oder verwaltete Dienste zu empfangen oder zu denen er Google den Zugriff gestattet, soweit anwendbar;
- Neue Absätze 7.3.1(d) und (e) werden folgendermaßen hinzugefügt:
 - d. Beschränkung der Menge der vom Kunden oder in dessen Auftrag an Google übermittelten Kundendaten auf ein Minimum; und
 - e. soweit der Zugriff von Google auf Kundendaten in der Kontrolle des Kunden liegt, diesen Zugriff zu widerrufen, sobald Google die Mandiant Consulting Services und/oder verwalteten Dienste abgeschlossen hat, sofern anwendbar.
- Anhang 2 (Sicherheitsmaßnahmen) wird folgendermaßen ersetzt:
 - Anhang 2: Zusätzliche technische und organisatorische Maßnahmen

1. Kundenkontrollierte Umgebung. Der Zugriff oder die Verarbeitung seitens Google erfolgt nur für Daten, die Google vom Kunden oder im Namen des Kunden über ein vom Kunden kontrolliertes oder genehmigtes Konto bzw. eine derartige Umgebung bereitgestellt wurden.

2. Datenzugriffsprozesse und -richtlinien – Zugriffsrichtlinien. Die Datenzugriffsprozesse und -richtlinien von Google sollen verhindern, dass unbefugte Personen und/oder Systeme Zugriff auf Systeme erhalten, die zur Verarbeitung von Kundendaten verwendet werden. Google (i) erlaubt Personen nur den Zugriff auf Daten, für die sie zugriffsberechtigt sind; und (ii) ergreift Maßnahmen, um sicherzustellen, dass Kundendaten während der Verarbeitung und Nutzung nicht ohne Autorisierung gelesen, kopiert, geändert oder entfernt werden können. Die Gewährung oder Änderung von Zugriffsrechten seitens Google geschieht auf der Grundlage der Bereitstellung des Endnutzerzugangs zu seinem Konto oder seiner Umgebung durch den Kunden an Google.

3. Mitarbeitersicherheit. Die Mitarbeiter von Google sind verpflichtet, sich in Übereinstimmung mit den Richtlinien des Unternehmens in Bezug auf Vertraulichkeit, Geschäftsethik, angemessene Nutzung und professionelle Standards zu verhalten. Google führt im angemessenen Umfang Hintergrundüberprüfungen durch, soweit dies im Einklang mit anwendbarem Recht, insbesondere mit anwendbarem, vor Ort geltendem Arbeitsrecht und anwendbaren gesetzlichen Bestimmungen steht.

Die Mitarbeiter sind verpflichtet, eine Vertraulichkeitsvereinbarung zu unterzeichnen sowie den Erhalt und die Einhaltung der Vertraulichkeits- und Datenschutzbestimmungen von Google zu bestätigen. Das Personal erhält eine Sicherheitsschulung. Mitarbeiter, die mit Kundendaten umgehen, müssen zusätzliche Anforderungen erfüllen, die ihrer Rolle entsprechen (z. B. Zertifizierungen). Mitarbeiter von Google verarbeiten Kundendaten nicht ohne Autorisierung.

4. Zusätzliche Sicherheitsmaßnahmen. Google und der Kunde können, soweit anwendbar, im jeweiligen Bestellformular, einschließlich einer beigefügten Leistungsbeschreibung, zusätzliche

Sicherheitsmaßnahmen für die Mandiant Consulting Services und/oder verwalteten Dienste vereinbaren.

2. Vom Kunden beauftragte Anbieter. Zur Klarstellung und ohne Einschränkung der Verpflichtungen von Google gemäß Absatz 7 (Datensicherheit) oder 11 (Unterauftragsverarbeiter) werden in Anhang 2 (Sicherheitsmaßnahmen) nicht die Sicherheitsmaßnahmen oder -kontrollen beschrieben, die vom Kunden oder vom Kunden beauftragten Anbietern umgesetzt oder bereitgestellt werden.

Implementierungsdienste

1. Weitere Definitionen.

- „Kundendaten“ bezeichnet Daten, für die der Kunde von Google beauftragten Personen Zugriff auf die vom Kunden verwalteten Systeme gewährt.
- „Vom Kunden verwaltetes System“ bezeichnet Folgendes, wie vom Kunden zum Empfang von Implementierungsdiensten verwendet: (a) vom Kunden verwaltete Instanzen von Google Cloud-Diensten oder Cloud-Diensten Dritter; und (b) jegliche Hardware oder Software, die in der lokalen Umgebung des Kunden gehostet oder verwaltet wird.
- „Google Cloud-Dienste“ bezeichnet alle in dieser Anlage 4 (Spezifische Produkte) beschriebenen Dienste, mit Ausnahme von Implementierungsdiensten, Mandiant Consulting Services und Mandiant Managed Services.
- „Mitarbeiter von Google“ bezeichnet Beschäftigte und Auftragnehmer von Google, die mit der Erbringung von Implementierungsdiensten beauftragt sind.
- „Implementierungsdienste“ bezeichnet Beratungs-, Consulting- und Implementierungsdienste, die von Beschäftigten und Auftragnehmern von Google zur Unterstützung von Google Cloud-Diensten gemäß der Vereinbarung, einschließlich eines Bestellformulars oder einer Leistungsbeschreibung, erbracht werden.

2. Änderungsvereinbarungen. Hinsichtlich Implementierungsdiensten gelten für diesen Zusatz folgende Änderungen:

- Die Definition von „Zusätzliche Sicherheitskontrollmaßnahmen“ wird gelöscht.
- Die Definition von „Datenvorfall“ wird folgendermaßen ersetzt:
 - „Datenvorfall“ bezeichnet eine Verletzung des Absatz 7.1 (Sicherheitsmaßnahmen, -kontrollen und -unterstützung von Google) durch Mitarbeiter von Google, der zur versehentlichen oder rechtswidrigen Vernichtung, zu Verlust, Änderung, unberechtigten Offenlegung von oder unberechtigtem Zugriff auf personenbezogene Kundendaten führt.
- Vorbehaltlich des übrigen vorliegenden Absatzes wird der Begriff „Kundendaten“ durch „personenbezogene Kundendaten“ ersetzt, wenn er (a) in Absatz 2 (Definitionen) in der

Definition von „Unterauftragsverarbeiter“ und (b) in anderen Absätzen dieses Zusatzes verwendet wird. Zur Klarstellung: Andere Definitionen in Absatz 2 (Definitionen) bleiben unverändert.

- Absatz 3 (Dauer) wird folgendermaßen ersetzt:
 - **3. Dauer.** Dieser Zusatz bleibt ungeachtet des Ablaufs der geltenden Vereinbarung in Kraft und erlischt automatisch, wenn Google keinen Zugriff mehr auf personenbezogene Kundendaten hat.
- Absatz 6 (Datenlöschung) wird folgendermaßen ersetzt:
 - **6. Datenlöschung.** Der Kunde wird am Ende der Laufzeit (a) entscheiden, ob personenbezogene Kundendaten gelöscht werden sollen; und wird (b) für eine solche Löschung verantwortlich sein.
- Der zweite Satz von Absatz 7.1.1 (Sicherheitsmaßnahmen von Google) wird folgendermaßen ersetzt:
 - „Die Sicherheitsmaßnahmen können (je nach Angemessenheit) Maßnahmen zur Verschlüsselung von Kundendaten umfassen, um die kontinuierliche Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste von Google zu gewährleisten, um nach einem Vorfall den zeitnahen Zugriff auf Kundendaten wiederherzustellen, und zur regelmäßigen Wirksamkeitsprüfung.“
- Absatz 7.1.3 (Zusätzliche Sicherheitskontrollmaßnahmen) wird gelöscht, ebenso wie alle anderen Verweise auf diesen Absatz.
- Absatz 9.1 (Zugriff; Berichtigung; Eingeschränkte Verarbeitung; Übertragbarkeit) wird folgendermaßen ersetzt:
 - *9.1 Zugriff; Berichtigung; eingeschränkte Verarbeitung; Übertragbarkeit.* Der Kunde ist dafür verantwortlich, die Funktionen der vom Kunden verwalteten Systeme zu nutzen, um auf die personenbezogenen Kundendaten zuzugreifen, sie zu berichtigen und ihre Verarbeitung einzuschränken, auch wenn der Kunde feststellt, dass personenbezogene Kundendaten falsch oder nicht mehr aktuell sind, und er nach anwendbarem Datenschutzrecht verpflichtet ist, diese Daten zu berichtigen oder zu löschen.
- Absatz 11.4 (Möglichkeit, dem Einsatz eines Unterauftragsverarbeiters zu widersprechen) wird folgendermaßen ersetzt:
 - *11.4 Möglichkeit, dem Einsatz eines Unterauftragsverarbeiters zu widersprechen.* Wenn während der Laufzeit ein neuer Unterauftragsverarbeiter beauftragt wird, benachrichtigt Google den Kunden über diese Beauftragung des neuen Unterauftragsverarbeiters, bevor dieser personenbezogene Kundendaten verarbeitet. Der Kunde kann dem neuen Unterauftragsverarbeiter widersprechen, indem er Google

benachrichtigt. In diesem Fall werden die Parteien nach Treu und Glauben zusammenarbeiten, um eine für beide Seiten akzeptable Alternative zu finden.

- Anhang 1 (Gegenstand und Details der Datenverarbeitung) wird folgendermaßen geändert:
 - Der Absatz „Dauer der Verarbeitung“ wird durch Folgendes ersetzt:
 - „*Dauer der Verarbeitung.* Die Laufzeit zuzüglich, soweit anwendbar, des Zeitraums vom Ende der Laufzeit bis zum Ablauf des Zugriffs auf personenbezogene Kundendaten.“
 - Die Formulierung „Google über die Dienste bereitgestellt“ in den Absätzen „Datenkategorien“ und „Betroffene Personen“ wird durch „Google im Zusammenhang mit den Diensten zugänglich gemacht“ ersetzt.
- Anhang 2 (Sicherheitsmaßnahmen) wird folgendermaßen ersetzt:
 - **Anhang 2: Sicherheitsmaßnahmen**

1. Vom Kunden verwaltete Systeme. Mitarbeiter von Google greifen nur auf den vom Kunden verwalteten Systemen auf die personenbezogenen Kundendaten zu und verarbeiten diese. Wenn diese Systeme Google Cloud-Dienste umfassen, unterliegt die Nutzung der Google Cloud-Dienste durch den Kunden weiterhin der für diese Dienste geltenden Vereinbarung.

2. Zugriffssteuerung. Die internen Datenzugriffsprozesse und -richtlinien von Google sollen verhindern, dass unbefugte Personen und Systeme Zugriff auf Google Cloud-Dienste erhalten, die zur Verarbeitung von personenbezogenen Daten verwendet werden. Google-Richtlinien (i) gestatten Mitarbeitern von Google nur den Zugriff auf Daten, für die sie eine Zugriffsberechtigung haben; und (ii) verpflichten die Mitarbeiter von Google, personenbezogene Kundendaten während der Verarbeitung, Nutzung und nach der Speicherung ohne entsprechende Berechtigung weder zu lesen, zu kopieren, zu verändern noch zu entfernen. Der Kunde kontrolliert die Bereitstellung oder Änderung von Endnutzer-Zugriffsrechten auf vom Kunden verwaltete Systeme. Wenn diese Systeme Google Cloud-Dienste umfassen, werden Einzelheiten zu Workflow-Tools, die Audit-Datensätze über Änderungen und Systemzugriffsprotokolle aufzeichnen, in der Vereinbarung für die entsprechenden Google Cloud-Dienste geregelt.

3. Mitarbeitersicherheit. Die Mitarbeiter von Google sind verpflichtet, sich in Übereinstimmung mit den Richtlinien des Unternehmens in Bezug auf Vertraulichkeit, Geschäftsethik, angemessene Nutzung und professionelle Standards zu verhalten. Google führt im angemessenen Umfang Hintergrundüberprüfungen durch, soweit dies im Einklang mit anwendbarem Recht, insbesondere mit anwendbarem, vor Ort geltendem Arbeitsrecht und anwendbaren gesetzlichen Bestimmungen steht.

Die Mitarbeiter von Google sind verpflichtet, eine Vertraulichkeitsvereinbarung zu unterzeichnen sowie den Erhalt und die Einhaltung der Vertraulichkeits- und Datenschutzbestimmungen von Google zu bestätigen. Mitarbeiter von Google erhalten eine

Sicherheitsschulung. Mitarbeiter von Google, die personenbezogene Kundendaten verarbeiten, müssen zusätzliche Auflagen erfüllen, die ihrer Rolle entsprechen (z. B. Zertifizierungen).

4. Zusätzliche Sicherheitsmaßnahmen. Google und der Kunde können in der Vereinbarung, einschließlich in einem Bestellformular oder einer Leistungsbeschreibung, zusätzliche Sicherheitsmaßnahmen vereinbaren.

5. Sicherheit von Unterauftragsverarbeitern. Vor dem Einsatz von Unterauftragsverarbeitern führt Google zuerst einen Audit ihres Umgangs mit der Sicherheit und dem Datenschutz durch, um dafür zu sorgen, dass ein Sicherheits- und Datenschutzniveau besteht, das im angemessenen Verhältnis zum Datenzugriff und dem Umfang der beauftragten Dienstleistungen steht. Nachdem Google die bestehenden Risiken der Zusammenarbeit mit einem Unterauftragsverarbeiter bewertet hat, muss dieser, unter Beachtung der in Absatz 11.3 (Anforderungen an den Einsatz von Unterauftragsverarbeitern) dargelegten Voraussetzungen, entsprechenden Vertragsbedingungen bezüglich Sicherheit, Vertraulichkeit und Datenschutz zustimmen.

3. Sicherheitspflichten des Kunden. Zusätzlich zu den Verpflichtungen in Absatz 7.3.1 (Sicherheitspflichten des Kunden) ist der Kunde für Folgendes verantwortlich:

- die Verwaltung, Zugriffsverwaltung und Sicherung der vom Kunden verwalteten Systeme, einschließlich der Minimierung des Zugriffs von Mitarbeitern von Google auf personenbezogene Kundendaten, soweit dies nach vernünftigem Ermessen möglich ist, sowie der Beendigung dieses Zugriffs nach Abschluss der Implementierungsdienste; und
- Umsetzung aller Sicherheitsempfehlungen, die Google dem Kunden in Bezug auf die vom Kunden verwalteten Systeme schriftlich mitgeteilt hat.

4. Compliance-Zertifizierung. Google wird Zertifikate für ISO 27001, ISO 27017 und ISO 27018 aufrechterhalten, die die im Rahmen der Google Cloud Platform und Google Workspace erbrachten Implementierungsleistungen (die „Compliance-Zertifizierungen für Implementierungsdienste“) abdecken. Google kann jederzeit Standards hinzufügen. Google kann eine Compliance-Zertifizierung für Implementierungsdienste durch eine gleichwertige oder verbesserte Alternative ersetzen.

5. Überprüfung der Compliance-Zertifizierung Um nachzuweisen, dass Google seinen Verpflichtungen aus dem vorliegenden Zusatz nachkommt, stellt Google dem Kunden die Compliance-Zertifizierung für Implementierungsdienste zur Einsichtnahme zur Verfügung und ermöglicht dem Kunden, sofern dieser als Auftragsverarbeiter handelt, den Antrag auf Zugang der betreffenden verantwortlichen Stelle zur Compliance-Zertifizierung für Implementierungsdienste.

6. Orte der Datenverarbeitung. Personenbezogene Kundendaten können in jedem Land verarbeitet werden, in dem Google Implementierungsdienste anbietet oder in dem der Kunde vom Kunden verwaltete Systeme unterhält.

7. Keine Angabepflicht für Kunden außerhalb von EMEA. Der Kunde ist nicht zur Angabe oder zur Identifizierung seiner zuständigen Aufsichtsbehörde verpflichtet, wie in Abschnitt 4.2 (Angabepflicht für

Kunden außerhalb von EMEA) der Bestimmungen unter „Europäisches Datenschutzrecht“ in Anhang 3 (Konkrete Datenschutzgesetze) für Implementierungsdienste beschrieben.

8. Informationen zu Unterauftragsverarbeitern. Unterauftragsverarbeiter für Implementierungsdienste werden (als Unterauftragnehmer) in einem anwendbaren Bestellformular, Leistungsbeschreibung oder einer sonstigen dem Kunden vor Beginn der Implementierungsdienste bereitgestellten Bestätigung benannt oder sind mit Google verbundene Unternehmen. Google stellt dem Kunden auf Anfrage auch Namen, Standorte und Aktivitäten von Unterauftragsverarbeitern für Implementierungsdienste zur Verfügung.

9. Verzeichnis von Verarbeitungstätigkeiten von Google. Soweit Google nach anwendbarem Datenschutzrecht verpflichtet ist, Datensätze mit bestimmten Kundeninformationen zu erheben und zu pflegen, stellt der Kunde Google auf Anfrage diese Informationen zur Verfügung und informiert Google über alle erforderlichen Aktualisierungen, um die Informationen korrekt und auf dem neuesten Stand zu halten, es sei denn, Google fordert den Kunden auf, solche Informationen über andere Methoden zur Verfügung zu stellen und zu aktualisieren.

Google Cloud Skills Boost für Organisationen

1. Weitere Definitionen.

- Sofern in der Vereinbarung nicht definiert, bezeichnet „Konto“ das Konto des Kunden für Google Cloud Skills Boost für Organisationen.
- „GCSBO“ bezeichnet Bildungs-, Schulungs- und Lerndienste und -inhalte, die über <https://www.cloudskillsboost.google/> (oder eine andere von Google betriebene und kontrollierte Website, die für die Zwecke von Google Cloud Skills Boost für Organisationen genutzt wird) bereitgestellt werden.
- „TSD“ bezeichnet technische Supportdienste, die Google nach eigenem Ermessen dem Kunden zur Verfügung stellen kann.

2. Änderungsvereinbarungen. Hinsichtlich GCSBO gelten für diesen Zusatz folgende Änderungen:

- Die Definition von „Zusätzliche Sicherheitskontrollmaßnahmen“ wird folgendermaßen ersetzt:
 - „Zusätzliche Sicherheitskontrollmaßnahmen“ bezeichnet Sicherheitsressourcen, Features, Funktionen und/oder Kontrollen (falls vorhanden), die der Kunde nach eigenem Ermessen verwenden kann, einschließlich (falls vorhanden) Verschlüsselung, Logging und Monitoring, Identitäts- und Zugriffsverwaltung und Sicherheitsscans.
- Die Definitionen von „Standardvertragsklauseln (Verantwortlicher an Auftragsverarbeiter)“, „Standardvertragsklauseln (Auftragsverarbeiter an Verantwortlichen)“, „Standardvertragsklauseln (Auftragsverarbeiter an Auftragsverarbeiter)“ und „Standardvertragsklauseln (Auftragsverarbeiter an Auftragsverarbeiter, Google-Exporteur)“ in Anhang 3 (Konkrete Datenschutzgesetze) werden folgendermaßen ersetzt:

- „Standardvertragsklauseln (Verantwortlicher an Auftragsverarbeiter)“ bezeichnet die Bestimmungen unter:
<https://cloud.google.com/terms/skillsboost-organizations/sccs/eu-c2p>;
- „Standardvertragsklauseln (Auftragsverarbeiter an Verantwortlichen)“ bezeichnet die Bestimmungen unter:
<https://cloud.google.com/terms/skillsboost-organizations/sccs/eu-p2c>;
- „Standardvertragsklauseln (Auftragsverarbeiter an Auftragsverarbeiter)“ bezeichnet die Bestimmungen unter:
<https://cloud.google.com/terms/skillsboost-organizations/sccs/eu-p2p>; and
- „Standardvertragsklauseln (Auftragsverarbeiter an Auftragsverarbeiter, Google-Exporteur)“ bezeichnet die Bestimmungen unter:
<https://cloud.google.com/terms/skillsboost-organizations/sccs/eu-p2p-intra-group>.

3. Standorte von Rechenzentren. Die Standorte der GCSBO-Rechenzentren werden beschrieben unter: <https://cloud.google.com/about/locations/>.

4. Keine Angabepflicht für Kunden außerhalb von EMEA. Der Kunde ist nicht zur Angabe oder zur Identifizierung seiner zuständigen Aufsichtsbehörde verpflichtet, wie in Absatz 4.2 (Angabepflicht für Kunden außerhalb von EMEA) der Bestimmungen unter „Europäisches Datenschutzrecht“ in Anhang 3 (Konkrete Datenschutzgesetze) für GCSBO beschrieben.

5. Informationen zu Unterauftragsverarbeitern. Die Namen, Standorte und Aktivitäten der GCSBO-Unterauftragsverarbeiter werden beschrieben unter:

- <https://cloud.google.com/terms/skillsboost-organizations/subprocessors> und
- <https://cloud.google.com/terms/subprocessors>.

6. Cloud-Datenschutzteam. Das Datenschutzteam für GCSBO kann unter <https://support.google.com/qwiklabs> (und/oder über andere von Google gelegentlich zur Verfügung gestellte Methoden) kontaktiert werden.

7. Verzeichnis von Verarbeitungstätigkeiten von Google. Soweit Google nach anwendbarem Datenschutzrecht verpflichtet ist, Datensätze mit bestimmten Kundeninformationen zu erheben und zu pflegen, stellt der Kunde Google auf Anfrage diese Informationen zur Verfügung und informiert Google über alle erforderlichen Aktualisierungen, um die Informationen korrekt und auf dem neuesten Stand zu halten, es sei denn, Google fordert den Kunden auf, solche Informationen über andere Methoden zur Verfügung zu stellen und zu aktualisieren.

Vorherige Versionen der Datenverarbeitungsbedingungen und Sicherheitsbestimmungen:

[9. April 2024](#) [30. Juni 2022](#) [24. September 2021](#) [19. August 2020](#) [10. August 2020](#) [17. Juli 2020](#)
[11. Oktober 2019](#) [1. Oktober 2019](#) [25. Mai 2018](#) [13. März 2018](#) [9. November 2017](#) [11. Oktober 2017](#)
[7. Februar 2017](#) [6. Oktober 2016](#)

Vorherige Versionen des Zusatzes zur Datenverarbeitung:

[7. Juli 2022](#) [24. September 2021](#) [27. Mai 2021](#) [29. Oktober 2019](#) [25. Mai 2018](#) [25. April 2018](#) [11. Juli 2017](#)
[28. November 2016](#) [7. Januar 2016](#) [24. April 2015](#) [1. April 2014](#) [14. November 2012](#)

Vorherige Versionen des Zusatzes zur Datenverarbeitung für Looker (Original)-Dienste (Kunden):

[14. Februar 2023](#) [4. Januar 2023](#) [20. September 2022](#) [30. Juni 2022](#) [16. März 2022](#) [24. September 2021](#)
[1. April 2021](#) [15. Januar 2021](#) [17. Dezember 2020](#) [28. August 2020](#) [1. Juni 2020](#) [9. März 2020](#)

Vorherige Versionen der Datenverarbeitungsbedingungen und Sicherheitsbestimmungen für SecOps-Dienste (Kunden):

[6. Februar 2023](#) [28. November 2022](#) [27. September 2021](#) [1. Oktober 2020](#)

Vorherige Versionen des Zusatzes zur Datenverarbeitung SecOps Consulting Services und verwaltete Dienste:

[5. Oktober 2023](#) [19. September 2023](#) [15. Juni 2023](#) [22. Februar 2023](#) [6. Februar 2023](#)

Vorherige Versionen (Zuletzt geändert am 15. Oktober 2024)

[26. September 2024](#) [9. September 2024](#) [5. August 2024](#) [23. Mai 2024](#) [9. April 2024](#) [8. November 2023](#)
[15. August 2023](#) [20. September 2022](#)