Auftragsdatenverarbeitungsbedingungen für Google Werbeprodukte

Google und die andere Vertragspartei, die diesen Bedingungen zustimmt (**„Kunde“**), haben einen Vertrag (in seiner jeweils gültigen Fassung) geschlossen, unter welchem die Auftragsverarbeiterdienste erbracht werden (die **„Vereinbarung”**).

Diese Auftragsdatenverarbeitungsbedingungen für Google Werbeprodukte (einschließlich mit den Anhängen nachfolgend als die **„Datenverarbeitungsbedingungen“** bezeichnet) werden zwischen Google und dem Kunden abgeschlossen und ergänzen die Vereinbarung. Diese Datenverarbeitungsbedingungen treten am Wirksamkeitsdatum in Kraft und ersetzen alle vorherigen Vereinbarungen zu dem gleichen Regelungsgegenstand (z.B. alle Änderungs- und Zusatzvereinbarungen zur Datenverarbeitung oder Regelungen zur Auftragsdatenverarbeitung).

Wenn Sie diese Datenverarbeitungsbedingungen stellvertretend für den Kunden abschließen, versichern Sie, dass Sie (a) rechtlich vollumfänglich dazu befugt sind, für den Kunden diese Datenverarbeitungsbedingungen stellvertretend abzuschließen, (b) diese Datenverarbeitungsbedingungen gelesen und verstanden haben und (c) für den von Ihnen vertretenen Kunden die Annahmeerklärung zum Abschluss dieser Datenverarbeitungsbedingungen abgeben. Wenn Sie rechtlich nicht dazu befugt sind, für den Kunden rechtsverbindliche Erklärungen abzugeben, schließen Sie diese Datenverarbeitungsbedingungen bitte nicht ab.

1. Einführung

Diese Datenverarbeitungsbedingungen enthalten die Vereinbarung der Vertragsparteien über die Regelungen, die für die Verarbeitung und Sicherheit von personenbezogenen Daten des Kunden im Zusammenhang mit den Datenschutzvorschriften gelten.

2. Begriffsbestimmungen und Auslegung

2.1 In diesen Datenverarbeitungsbedingungen gelten die folgenden Begriffsbestimmungen:

„Aufsichtsbehörde” bedeutet, je nach Anwendbarkeit, (a) die “Aufsichtsbehörde” wie sie in der EU DSGVO festgelegt ist und/oder (b) der “Commissioner” wie er in der UK DSGVO festgelegt wird.

„Auftragsverarbeiterdienste” bedeutet die jeweils einschlägigen Dienste, die unter privacy.google.com/businesses/adsservices aufgeführt sind.

„Datenschutzvorschriften“ bedeutet, soweit anwendbar: (a) die DSGVO und/oder (b) das Bundesgesetz über den Datenschutz (der Schweiz) von 1992.

„Datenvorfall“ bedeutet ein Sicherheitsvorkommnis bei Google, das zur/zum unabsichtlichen oder gesetzwidrigen Vernichtung, Verlust, Änderung von personenbezogenen Daten des Kunden oder zur unautorisierten Offenlegung oder zum unautorisierten Zugriff auf diese führt, wobei dabei Systeme betroffen sind, die von Google verwaltet oder anderweitig von Google kontrolliert werden. Nicht unter den Begriff „Datenvorfall” fallen erfolglose Zugriffsversuche oder ähnliche Ereignisse, die die Sicherheit der personenbezogenen Daten des Kunden nicht kompromittieren, wie etwa erfolglose Anmeldeversuche, Pings, Port-Scans, Denial-of-Service-Angriffe und andere Netzwerkangriffe auf Firewalls oder vernetzte Systeme.

„Drittanbieter-Unterauftragsverarbeiter“ hat die in Ziffer 11.1 (Zustimmung zur Verpflichtung von Unterauftragsverarbeitern) enthaltene Bedeutung.

„DSGVO“ bedeutet, je nach Anwendbarkeit, (a) die EU DSGVO und/oder (b) die UK DSGVO.

„E-Mail-Adresse für Benachrichtigungen“ bedeutet die E-Mail-Adresse (falls vorhanden), die vom Kunden über die Benutzeroberfläche des Auftragsverarbeiterdienstes oder über andere von Google bereitgestellte Möglichkeiten angegeben wurde, um bestimmte Benachrichtigungen von Google zu diesen Datenverarbeitungsbedingungen zu erhalten.

„EWR“ bedeutet der Europäische Wirtschaftsraum.

„EU DSGVO“ bedeutet 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 oder nationales Recht“ bedeutet, je nach Anwendbarkeit, (a) europäisches Recht oder das Recht eines Mitgliedstaates der Europäischen Union (wenn die EU DSGVO auf die Verarbeitung von personenbezogenen Daten des Kunden Anwendung findet), und/oder (b) das Recht des Vereinigten Königreichs oder eines Teils des Vereinigten Königreichs (wenn die UK DSGVO auf die Verarbeitung von personenbezogen Daten des Kunden Anwendung findet).

„Google-Gruppenunternehmen Unterauftragsverarbeiter“ hat die in Ziffer 11.1 (Zustimmung zum Einsatz von Unterauftragsverarbeitern) festgelegte Bedeutung.

„Google-Gruppenunternehmen“ bedeutet Google LLC (vormalige Bezeichnung Google Inc.), Google Ireland Limited oder andere verbundene Unternehmen der Google LLC.

„Google“ bedeutet das Google-Gruppenunternehmen, das Vertragspartei der Vereinbarung ist.

„ISO-27001-Zertifizierung“ bedeutet die Zertifizierung nach ISO/IEC 27001:2013 oder eine vergleichbare Zertifizierung der Auftragsverarbeiterdienste.

„Laufzeit“ bedeutet den Zeitraum zwischen dem Wirksamkeitsdatum und dem Ende der Erbringung der Auftragsverarbeiterdienste durch Google gemäß der Vereinbarung.

„Personenbezogene Daten des Kunden“ bedeutet personenbezogene Daten, die im Auftrag des Kunden durch Google im Rahmen der Erbringung der Auftragsverarbeiterdienste verarbeitet werden.

„Privacy Shield“ bedeutet das EU-US-Privacy-Shield-Rahmenprogramm, das Swiss-US Privacy Shield-Rahmenprogramm und ein vergleichbares Rahmenprogramm, das ggf. zwischen dem Vereinigten Königreich und den Vereinigten Staaten zur Anwendung kommt.

„Sicherheitsdokumentation“ bedeutet das Zertifikat, das für die ISO-27001-Zertifizierung ausgestellt wurde und jegliche anderen Sicherheitszertifizierungen oder Dokumentationen, die Google in Bezug auf die Auftragsverarbeiterdienste ggf. zur Verfügung stellt.

„Sicherheitsmaßnahmen“ hat die in Ziffer 7.1.1 (Googles Sicherheitsmaßnahmen) festgelegte Bedeutung.

„Tool für betroffene Personen“ bedeutet ein von einem Google-Gruppenunternehmen zur Verfügung gestelltes Tool (soweit jeweils vorhanden), das Google ermöglicht, direkt und auf standardisierte Weise bestimmte Anfragen von betroffenen Personen in Bezug auf personenbezogene Daten des Kunden zu beantworten (z. B. in Bezug auf Online-Einstellungen für Werbung oder ein Opt-out-Browser-Plugin).

„UK DSGVO“ bedeutet die EU DSGVO in der Fassung, wie sie ggf. mit Änderungen und durch die Umsetzung in das Recht des Vereinigten Königreichs gemäß dem UK European Union (Withdrawal) Act 2018 in Kraft tritt.

„Unterauftragsverarbeiter“ bedeutet Dritte, die unter diesen Datenverarbeitungsbedingungen autorisiert sind, logisch auf personenbezogene Daten des Kunden zuzugreifen und diese zu verarbeiten, um Teile der Auftragsverarbeiterdienste bereitzustellen und dazugehörigen technischen Support zu erbringen.

„Verbundenes Unternehmen“ bedeutet jede juristische Person, die direkt oder indirekt kontrolliert, von einer der Vertragsparteien kontrolliert wird oder unter gemeinsamer Kontrolle mit einer der Vertragsparteien steht.

„Wirksamkeitsdatum“ bedeutet entweder.

(a) der 25. Mai 2018, falls der Kunde im Rahmen eines ‚Click-to-Accept“-Verfahrens diese Datenverarbeitungsbedingungen oder die Vertragsparteien anderweitig die vorliegenden Datenverarbeitungsbedingungen an dem vorgenannten Datum oder zuvor geschlossen hat bzw. abgeschlossen haben, oder

(b) das Datum, an dem der Kunde im Rahmen eines ‚Click-to-Accept’-Verfahrens diese Datenverarbeitungsbedingungen abgeschlossen hat oder die Vertragsparteien anderweitig den vorliegenden Datenverarbeitungsbedingungen zugestimmt haben, falls dieses jeweils nach dem 25. Mai 2018 geschieht.

„Zusatzprodukt“ bedeutet ein Produkt, einen Dienst oder eine Anwendung von Google oder einem Dritten, das/der/die (a) nicht Bestandteil der Auftragsverarbeiterdienste ist und (b) zur Nutzung über die Benutzeroberfläche der Auftragsverarbeiterdienste erreichbar oder anderweitig in die Auftragsverarbeiterdienste integriert ist.

2.2 Die Begriffe **„Verantwortlicher“**, **„betroffene Person“**, **„personenbezogene Daten“**, **„Verarbeitung“** und **„Auftragsverarbeiter“** haben in diesen Datenverarbeitungsbedingungen jeweils dieselbe Bedeutung, die ihnen in der DSGVO zugewiesen wird.

2.3 Formulierungen, die mit Worten wie **„einschließlich“** oder mit einem ähnlichen Ausdruck beginnen, sind so auszulegen, dass diese Formulierungen nur illustrativ gemeint sind und sie die Bedeutung der davorstehenden Formulierungen nicht einschränken sollen. Etwaige in diesen Datenverarbeitungsbedingungen angeführte Beispiele dienen nur der Veranschaulichung und sind

nicht als ausschließliche Beispiele für ein bestimmtes Konzept gemeint.

2.4 Verweise auf Gesetze oder gesetzliche Regelungen beziehen sich jeweils auf deren aktuellen Stand und deren zum jeweiligen Zeitpunkt gültige und ggf. geänderte oder überarbeitete Fassung.

3. Laufzeit dieser Datenverarbeitungsbedingungen

Die vorliegenden Datenverarbeitungsbedingungen treten zum angegebenen Wirksamkeitsdatum in Kraft und bleiben – unabhängig davon, ob die Laufzeit abgelaufen sein sollte – solange in Kraft, bis Google alle personenbezogenen Kundendaten gemäß den vorliegenden Datenverarbeitungsbedingungen gelöscht hat; zu diesem Zeitpunkt enden diese Datenverarbeitungsbedingungen automatisch.

4. Anwendbarkeit dieser Datenverarbeitungsbedingungen

4.1 **Anwendbarkeit der Datenschutzvorschriften.** Diese Datenverarbeitungsbedingungen gelten nur in dem Umfang, in dem die Datenschutzvorschriften auf die Verarbeitung personenbezogener Daten des Kunden Anwendung finden, einschließlich wenn:

(a) die Verarbeitung im Rahmen der Tätigkeiten einer Betriebsstätte des Kunden im EWR oder im Vereinigten Königreich stattfindet und/oder

(b) personenbezogene Daten des Kunden personenbezogene Daten darstellen, die sich auf betroffene Personen beziehen, die sich im EWR oder im Vereinigten Königreich befinden und sich die Verarbeitung auf das Angebot von Waren oder Dienstleistungen oder die Beobachtung des Verhaltens im EWR oder im Vereinigten Königreich bezieht.

4.2 **Anwendbarkeit auf Auftragsverarbeiterdienste.** Diese Datenverarbeitungsbedingungen gelten nur für solche Auftragsverarbeiterdienste, für welche die Vertragsparteien diese Datenverarbeitungsbedingungen abgeschlossen haben (zum Beispiel, für solche Auftragsverarbeiterdienste, (a) für die der Kunde diese Datenverarbeitungsbedingungen mittels eines 'Click-to-Accept'-Verfahrens abgeschlossen hat oder (b) auf die die Vereinbarung Anwendung findet und in welche diese Datenverarbeitungsbedingungen einbezogen und zum Gegenstand der Vereinbarung gemacht werden).

5. Verarbeitung von Daten

5.1 **Rollenverteilung und Einhaltung gesetzlicher Vorgaben; Autorisierung.**

5.1.1 **Verantwortlichkeiten des Auftragsverarbeiters und des Verantwortlichen.** Die Vertragsparteien bestätigen und vereinbaren, dass:

(a) Anhang 1 den Gegenstand und die Details der Verarbeitung der personenbezogenen Daten des Kunden beschreibt,

(b) Google als ein Auftragsverarbeiter von personenbezogenen Daten des Kunden gemäß den Datenschutzvorschriften handelt,

(c) der Kunde, je nachdem was zutrifft, als ein Verantwortlicher oder ein Auftragsverarbeiter von personenbezogenen Daten des Kunden gemäß den Datenschutzvorschriften handelt, und

(d) jede Vertragspartei verpflichtet ist, den Verpflichtungen nachzukommen, die für die jeweilige Partei in Bezug auf die Verarbeitung von personenbezogenen Daten des Kunden gemäß den Datenschutzvorschriften gelten.

5.1.2 **Autorisierung durch einen Dritten als Verantwortlichen.** Ist der Kunde selbst ein Auftragsverarbeiter, so sichert er gegenüber Google zu, dass seine Weisungen und Maßnahmen hinsichtlich personenbezogener Daten des Kunden, einschließlich der Einsetzung von Google als weiteren Auftragsverarbeiter, durch den betreffenden Verantwortlichen autorisiert wurden.

5.2 **Weisungen des Kunden.** Durch Zustimmung zu diesen Datenverarbeitungsbedingungen weist der Kunde Google an, personenbezogene Daten des Kunden in Übereinstimmung mit dem anwendbaren Recht zu verarbeiten, (a) um die Auftragsverarbeiterdienste und damit im Zusammenhang stehenden technischen Support zu erbringen, und (b) wie weiter

durch die Nutzung des Kunden der Auftragsverarbeiterdienste festgelegt (einschließlich durch die Einstellungen und Funktionalitäten der Auftragsverarbeiterdienste) und damit im Zusammenhang stehenden technischen Support, (c) wie durch die Vereinbarung, einschließlich dieser Datenverarbeitungsbedingungen, dokumentiert wird und (d) wie zusätzlich in anderen schriftlichen Weisungen dokumentiert ist, die vom Kunden gegeben wurden und von Google förmlich als Weisung im Sinne der vorliegenden Datenverarbeitungsbedingungen anerkannt wurden.

5.3 **Befolgung der Weisungen durch Google.** Google wird die Weisungen, die in Ziffer 5.2 (Weisungen des Kunden) festgelegt sind (auch im Hinblick auf die Übermittlung von Daten) befolgen, es sei denn, europäisches oder nationales Recht, das auf Google Anwendung findet, erfordert eine anderweitige Verarbeitung der personenbezogenen Daten des Kunden durch Google; in einem solchen Fall wird Google den Kunden entsprechend informieren (es sei denn, das jeweilige Recht verbietet Google dies aus wichtigen Gründen des öffentlichen Interesses zu tun).

5.4 **Zusatzprodukte.** Wenn der Kunde Zusatzprodukte verwendet, können die Auftragsverarbeiterdienste diesen Zusatzprodukten den Zugriff auf personenbezogene Daten des Kunden ermöglichen, sofern dies für die Interaktion zwischen diesen Zusatzprodukten und den Auftragsverarbeiterdiensten erforderlich ist. Zur Klarstellung, diese Datenverarbeitungsbedingungen gelten nicht für die Verarbeitung von personenbezogenen Daten im Zusammenhang mit der Bereitstellung von Zusatzprodukten, die durch den Kunden genutzt werden, einschließlich für personenbezogene Daten, die von oder zu diesen Zusatzprodukten übermittelt werden.

6. Löschung von Daten

6.1 **Löschung während der Laufzeit.**

6.1.1 **Auftragsverarbeiterdienste mit Löschfunktion.** Falls während der Laufzeit:

(a) die Softwarefunktionalitäten der Auftragsverarbeiterdienste dem Kunden eine Möglichkeit zur Verfügung stellen, personenbezogene Daten des Kunden zu löschen,

(b) der Kunde die Auftragsverarbeiterdienste dazu nutzt, bestimmte personenbezogene Daten des Kunden zu löschen und

(c) die gelöschten personenbezogenen Daten des Kunden vom Kunden nicht wiederhergestellt werden können (z. B. aus dem ‚Papierkorb'),

dann wird Google diese personenbezogenen Daten des Kunden von ihren Systemen so früh wie es angemessen und praktikabel ist und spätestens nach einer Dauer von 180 Tagen löschen, falls nicht europäisches oder nationales Recht eine Aufbewahrung vorschreibt.

6.1.2 **Auftragsverarbeiterdienste ohne Löschfunktion.** Falls die Softwarefunktionalitäten der Auftragsverarbeiterdienste keine Möglichkeit vorsehen die den Kunden in die Lage versetzt, während der Laufzeit personenbezogene Daten des Kunden zu löschen, dann wird Google:

(a) jeder angemessenen Anfrage des Kunden entsprechen, um eine solche Löschung zu erreichen, soweit dies unter Berücksichtigung der Art und Funktionsweise der Auftragsverarbeiterdienste möglich ist und falls nicht europäisches oder nationales Recht eine Aufbewahrung vorschreibt, und

(b) die Datenspeicherungsverfahren, die unter policies.google.com/technologies/ads beschrieben sind, einhalten.

Google ist berechtigt, einen Ersatz der Kosten (basierend aufs Googles angemessenen Aufwendungen) für die Löschung von Daten nach Ziffer 6.1.2(a) zu verlangen. Vor einer solchen Löschung wird Google dem Kunden weitere Details zu den jeweils entstehenden Kosten und die Grundlage für die Berechnung dieser Kosten zur Verfügung stellen.

6.2 **Löschung nach Ablauf der Laufzeit.** Der Kunde weist Google an, nach Ablauf der Laufzeit sämtliche personenbezogenen Daten des Kunden (einschließlich aller existierenden Kopien) gemäß den Vorgaben des anwendbaren Rechts von Googles Systemen zu löschen. Google wird dieser Weisung so früh wie es angemessen und praktikabel ist und spätestens nach einer Dauer von 180 Tagen Folge leisten, falls nicht europäisches oder nationales Recht eine Aufbewahrung vorschreibt.

7. Datensicherheit

7.1 **Sicherheitsmaßnahmen und Hilfestellung durch Google.**

7.1.1 **Googles Sicherheitsmaßnahmen.** Google implementiert technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten des Kunden vor versehentlicher oder gesetzeswidriger Zerstörung, Verlust, Veränderung, unbefugter Offenlegung oder unbefugtem Zugriff, wie in Anhang 2 beschrieben (die **„Sicherheitsmaßnahmen"**) und

erhält diese aufrecht. Wie in Anhang 2 beschrieben, beinhalten die Sicherheitsmaßnahmen Maßnahmen: (a) zur Verschlüsselung personenbezogener Daten, (b) die helfen, die Vertraulichkeit, Integrität, Verfügbarkeit und Ausfallsicherheit von Googles Systemen und Diensten fortwährend zu wahren bzw. sicherzustellen, (c) die helfen, zeitgerecht den Zugang zu personenbezogenen Daten nach einem Vorfall wiederherzustellen und (d) um regelmäßig die Wirksamkeit zu testen. Google kann gelegentlich die Sicherheitsmaßnahmen aktualisieren oder anpassen, sofern eine solche Aktualisierung und Anpassung nicht zu einer Verschlechterung der Gesamtsicherheit der Auftragsverarbeiterdienste führt.

7.1.2 **Einhaltung von Sicherheitsvorschriften durch Googles Personal.** Google ist verpflichtet, angemessene Maßnahmen zu ergreifen, um die Einhaltung der Sicherheitsmaßnahmen durch Google-Mitarbeiter, Auftragnehmer und Unterauftragsverarbeiter in dem Umfang sicherzustellen, wie es für deren jeweiliges Aufgabengebiet angemessen ist, und um sicherzustellen, dass sich sämtliche Personen, die autorisiert sind, personenbezogene Daten des Kunden zu verarbeiten, zur Geheimhaltung verpflichtet haben oder entsprechenden gesetzlichen Geheimhaltungspflichten unterliegen.

7.1.3 **Hilfestellung durch Google.** Der Kunde ist damit einverstanden, dass Google (unter Berücksichtigung der Art der jeweiligen Verarbeitung personenbezogener Daten des Kunden und der Informationen, die Google zur Verfügung stehen) den Kunden bei der die Einhaltung von sämtlichen Pflichten des Kunden in Bezug auf die Sicherheit von personenbezogenen Daten und bei Verletzung der Datensicherheit, einschließlich, soweit anwendbar, die Pflichten des Kunden gemäß den Artikeln 32 bis 34 DSGVO, unterstützt durch:

(a) Implementierung und Aufrechterhaltung von Sicherheitsmaßnahmen in Übereinstimmung mit Ziffer 7.1.1 (Googles Sicherheitsmaßnahmen),

(b) Einhaltung der Regelungen in Ziffer 7.2 (Datenvorfälle) und

(c) Bereitstellung von Sicherheitsdokumentationen an den Kunden gemäß Ziffer 7.5.1 (Überprüfungen der Sicherheitsdokumentation) und den Informationen, die in diesen Datenverarbeitungsbedingungen enthalten sind.

7.2 **Datenvorfälle.**

7.2.1 **Meldung von Datenvorfällen.** Falls Google Kenntnis von einem Datenvorfall erlangen sollte, ist Google verpflichtet: (a) den Kunden unverzüglich den Datenvorfall zu melden; und (b) prompt angemessene Maßnahmen zur Schadensminimierung und Sicherung der personenbezogenen Daten des Kunden zu ergreifen.

7.2.2 **Detailinformationen zu Datenvorfällen.** Meldungen gemäß 7.2.1 (Googles Sicherheitsmaßnahmen) enthalten, soweit wie möglich, Details über den Datenvorfall und Informationen darüber, welche Maßnahmen ergriffen wurden, um das potenzielle Risiko zu minimieren und welche Schritte Google dem Kunden empfiehlt, um auf den Datenvorfall zu reagieren.

7.2.3 **Übermittlung der Meldungen.** Meldungen über Datenvorfälle wird Google an die E-Mail-Adresse für Benachrichtigungen senden, oder nach Googles Ermessen (z.B. falls der Kunde keine E-Mail-Adresse für Meldungen angegeben hat) mittels eines anderen direkten Kommunikationsmittels (z.B. mittels Telefon oder in einem persönlichen Treffen) übermitteln. Der Kunde trägt die alleinige Verantwortung, die E-Mail-Adresse für Benachrichtigungen zu benennen, und hat sicherzustellen, dass die E-Mail-Adresse für Benachrichtigungen stets aktuell und gültig ist.

7.2.4 **Meldungen an Dritte.** Der Kunde trägt die alleinige Verantwortung, gesetzliche Vorgaben für Meldungen bei Vorfällen einzuhalten und entsprechenden Meldepflichten bei Datenvorfällen gegenüber Dritten nachzukommen.

7.2.5 **Kein Anerkenntnis durch Google.** Die Meldung eines Datenvorfalls durch Google bzw. die Reaktion auf einen Datenvorfall durch Google gemäß dieser Ziffer 7.2 (Datenvorfälle) kann nicht dahingehend ausgelegt werden, dass Google dadurch bereits ein Fehlverhalten einräumen oder die Haftung für den Datenvorfall anerkennen würde.

7.3 **Verantwortlichkeit des Kunden für Sicherheit und Sicherheitsbewertung.**

7.3.1 **Verantwortlichkeit des Kunden für Sicherheit.** Unbeschadet der Verpflichtungen für Google gemäß Ziffern 7.1 (Sicherheitsmaßnahmen und Hilfestellung von Google) und 7.2 (Datenvorfälle):

(a) trägt der Kunde die alleinige Verantwortung für die Nutzung der Auftragsverarbeiterdienste, einschließlich:

(i) die Auftragsverarbeiterdienste in angemessener Art und Weise zu nutzen, um ein Sicherheitsniveau sicherzustellen, das im Verhältnis zum Risiko im Hinblick auf die Verarbeitung personenbezogenen Daten des Kunden angemessen ist und

(ii) die Anmeldeinformationen für die Authentifizierung sowie der Systeme und Geräte, die der Kunde

verwendet, um auf die Auftragsverarbeiterdienste zuzugreifen, zu schützen, und

(b) ist Google nicht dafür verantwortlich, personenbezogene Daten des Kunden zu schützen, bei denen der Kunde entscheidet, diese außerhalb der Google-Systeme oder der Systeme der Google-Unterauftragsverarbeiter zu speichern oder zu übermitteln.

7.3.2 **Sicherheitsbeurteilung durch den Kunden.** Der Kunde nimmt zur Kenntnis und stimmt zu, dass (unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung personenbezogener Daten des Kunden sowie der damit verbundenen Risiken für Einzelpersonen) die von Google gemäß Ziffer 7.1.1 (Googles Sicherheitsmaßnahmen) umgesetzten und aufrechterhaltenen Sicherheitsmaßnahmen ein Sicherheitsniveau erreichen, das mit den Risiken in Bezug auf die Verarbeitung der personenbezogenen Daten des Kunden in einem angemessenen Verhältnis steht.

7.4 **Sicherheitszertifizierung.** Um fortlaufend die Effektivität der Sicherheitsmaßnahmen zu bewerten und sicherzustellen, wird Google die ISO-27001-Zertifizierung aufrechterhalten.

7.5 **Prüfungen und Compliance-Audits.**

7.5.1 **Prüfung der Sicherheitsdokumentation.** Um die Einhaltung von Googles Verpflichtungen unter diesen Datenverarbeitungsbedingungen nachzuweisen, ist Google verpflichtet, die Sicherheitsdokumentation dem Kunden zur Prüfung zugänglich zu machen.

7.5.2 **Prüfrechte des Kunden.**

(a) Google wird dem Kunden oder einem unabhängigen, vom Kunden benannten Prüfer unter Maßgabe von Ziffer 7.5.3 (zusätzliche Bedingungen für Audits) ermöglichen, Audits (einschließlich Inspektionen) durchzuführen, um zu verifizieren, dass Google seinen Pflichten unter den Datenverarbeitungsbedingungen nachkommt. Google wird solche Audits, wie in Ziffer 7.4 (Sicherheitszertifizierung) und in dieser Ziffer 7.5 (Prüfungen und Compliance-Audits) beschrieben, unterstützen.

(b) Der Kunde kann auch ein Audit durchführen, indem er das ISO-27001-Zertifikat überprüft (welches das Ergebnis eines Audits widerspiegelt, das von einem unabhängigen Prüfer durchgeführt wurde), um zu verifizieren, dass Google seinen Pflichten unter den vorliegenden Datenverarbeitungsbedingungen nachkommt.

7.5.3 **Zusätzliche Bedingungen für Audits.**

(a) Der Kunde ist verpflichtet, eine Anfrage für ein Audit nach Ziffer 7.5.2(a) in Übereinstimmung mit Ziffer 12.1 (Kontaktaufnahme mit Google) zu stellen.

(b) Nach Erhalt einer Anfrage gemäß Ziffer 7.5.3(a) werden Google und der Kunde im Voraus gemeinsam ein angemessenes Startdatum, den Umfang und die Dauer und Sicherheits- und Vertraulichkeitsmaßnahmen, die Gegenstand des jeweiligen Audits gemäß Ziffer 7.5.2(a) sind, besprechen und vereinbaren.

(c) Google ist berechtigt, einen Ersatz der Kosten (basierend auf Googles angemessenen Aufwendungen) für jedes Audit nach Ziffer 7.5.2(a) zu verlangen. Vor jedem Audit wird Google dem Kunden weitere Details zu den jeweils entstehenden Kosten und die Grundlage für die Berechnung dieser Kosten zur Verfügung stellen. Jegliche Kosten, die für die Beauftragung und Durchführung eines Audits durch einen unabhängigen Prüfer entstehen, den der Kunde beauftragt hat, sind allein vom Kunden zu tragen.

(d) Google ist berechtigt, einen vom Kunden zur Durchführung eines Audits nach Ziffer 7.5.2(a) beauftragten unabhängigen Prüfer abzulehnen, wenn dieser Prüfer nach Googles angemessener Einschätzung nicht hinreichend qualifiziert oder unabhängig ist, es sich um einen Wettbewerber von Google handelt oder dieser aus anderen Gründen offenkundig ungeeignet ist. Falls Google einen solchen Einwand erhebt, ist der Kunde verpflichtet, einen anderen Prüfer zu bestellen oder das Audit selbst durchführen.

(e) Google ist nach diesen Datenverarbeitungsbedingungen nicht verpflichtet, dem Kunden oder einem vom Kunden beauftragten unabhängigen Prüfergegenüber das Folgende offenzulegen bzw. dem Kunden oder einem unabhängigen Prüfer zu gestatten, auf Folgendes zuzugreifen:

(i) Daten von irgendeinem anderen Kunden eines Google-Gruppenunternehmens;

(ii) interne Daten des Rechnungswesens oder Finanzinformationen eines Google-Gruppenunternehmens;

(iii) Geschäftsgeheimnisse eines Google-Gruppenunternehmens;

(iv) Informationen, die nach Googles angemessener Einschätzung (A) die Sicherheit von Systemen oder

Betriebsstätten eines Google-Gruppenunternehmens gefährden könnten oder (B) dazu führen könnten, dass ein Google-Gruppenunternehmen seine Pflichten unter den Datenschutzvorschriften verletzt oder gegen seine Sicherheits- bzw. Datenschutzverpflichtungen gegenüber dem Kunden oder Dritten verstößt; oder

(v) Informationen, auf die der Kunde oder sein unabhängiger Prüfer aus treuwidrigen Gründen, die nicht zur Erfüllung der Verpflichtungen des Kunden gemäß den Datenschutzvorschriften erforderlich sind, zugreifen möchten.

8. Folgenabschätzungen und Konsultationen

Der Kunde ist damit einverstanden, dass Google (unter Berücksichtigung der Art der Verarbeitung und der Informationen, die Google zur Verfügung stehen) den Kunden bei der Erfüllung seiner Pflichten zu Datenschutz-Folgenabschätzungen und vorherigen Konsultationen, einschließlich, soweit anwendbar, den Pflichten gemäß Art. 35 und 36 DSGVO; durch Folgendes unterstützt:

(a) Bereitstellung der Sicherheitsdokumentation gemäß Ziffer 7.5.1 (Prüfung der Sicherheitsdokumentation);

(b) Bereitstellung der Informationen, die bereits in diesen Datenverarbeitungsbedingungen enthalten sind; und

(c) Bereitstellung oder anderweitige Zugänglichmachung in Übereinstimmung mit Googles Standardverfahren von anderen Materialien (zum Beispiel Hilfeartikel im Hilfe-Center) zur Art der Auftragsverarbeiterdienste oder der Verarbeitung von personenbezogenen Daten des Kunden.

9. Rechte betroffener Personen

9.1 **Beantwortung von Anfragen betroffener Personen.** Wenn Google eine Anfrage von einer betroffenen Person hinsichtlich personenbezogener Daten des Kunden erhält, wird Google:

(a) direkt auf die Anfrage der betroffenen Person in Übereinstimmung mit den Standard-Funktionen eines Tools für betroffene Personen antworten, sollte die Anfrage über das Tool für betroffene Personen gestellt werden, oder

(b) die betroffene Person bitten, ihre Anfrage an den Kunden zu übermitteln, falls die Anfrage nicht über ein Tool für betroffene Personen eingereicht wurde; der Kunde trägt die alleinige Verantwortung für die Beantwortung einer solchen Anfrage.

9.2 **Unterstützung durch Google bei Anfragen betroffener Personen.** Der Kunde ist damit einverstanden, dass Google (unter Berücksichtigung der Art der Verarbeitung personenbezogener Daten des Kunden und, falls anwendbar, von Artikel 11 DSGVO) den Kunden bei der Erfüllung seiner Verpflichtungen unterstützen wird, auf Anfragen von betroffenen Personen zu antworten, einschließlich, falls anwendbar, auf Anfragen, die die Rechte der betroffenen Personen nach dem dritten Kapitel der DSGVO betreffen, indem Google:

(a) die Funktionalitäten der Auftragsverarbeiterdienste bereitstellt,

(b) die in Ziffer 9.1 (Beantwortung von Anfragen betroffener Personen) festgelegten Verpflichtungen erfüllt, und

(c) Tools für betroffene Personen bereitstellt, soweit dies für den jeweiligen Auftragsverarbeiterdienst zutreffend ist.

10. Datenübermittlungen

10.1 **Datenspeicherungs- und Datenverarbeitungseinrichtungen.** Der Kunde stimmt zu, dass Google vorbehaltlich Ziffer 10.2 (Datenübermittlungen) personenbezogene Daten des Kunden in den Vereinigten Staaten von Amerika oder in jedem anderen Land, in dem Google oder Googles Unterauftragsverarbeiter Einrichtungen unterhalten, speichern und verarbeiten kann.

10.2 **Datenübermittlungen.** Google wird sicherstellen, dass:

(a) die Muttergesellschaft der Google-Konzerngruppe, die Google LLC, gemäß den Privacy-Shield-Grundsätzen zertifiziert bleibt; und

(b) der Umfang der Privacy-Shield-Zertifizierung der Google LLC die personenbezogenen Daten des Kunden erfasst.

10.3 **Informationen zu Rechenzentren.** Informationen über die Standorte der Rechenzentren von Google können unter www.google.com/about/datacenters/inside/locations/index.html abgerufen werden.

11. Unterauftragsverarbeiter

11.1 **Genehmigung der Beauftragung von Unterauftragsverarbeitern.** Der Kunde genehmigt ausdrücklich die Beauftragung von verbundenen Unternehmen von Google als Unterauftragsverarbeiter (**„Google Gruppen-Unterauftragsverarbeiter“**). Zudem genehmigt der Kunde generell, dass Google auch Dritte als Unterauftragsverarbeiter beauftragen darf (**„Dritt-Unterauftragsverarbeiter“**).

11.2 **Informationen zu Unterauftragsverarbeitern.** Informationen über Unterauftragsverarbeiter können unter privacy.google.com/businesses/subprocessors abgerufen werden.

11.3 **Anforderungen für die Beauftragung von Unterauftragsverarbeitern.** Wenn Google Unterauftragsverarbeiter beauftragt, wird Google:

(a) durch schriftlichen Vertrag sicherstellen, dass:

(i) der Unterauftragsverarbeiter nur auf personenbezogene Daten des Kunden in dem Umfang zugreift und diese nutzt, wie dies erforderlich ist, um seine Obliegenheiten, zu denen er im Wege der Unterauftragsvergabe verpflichtet ist, zu erfüllen und dies jeweils unter Einhaltung der Vereinbarung (einschließlich dieser Datenverarbeitungsbedingungen) und dem Privacy-Shield erfolgt, und

(ii) die in Art. 28 Abs. 3 DSGVO festgelegten Datenschutzpflichten dem Unterauftragsverarbeiter auferlegt werden, falls die DSGVO auf die Verarbeitung der personenbezogenen Daten des Kunden Anwendung findet, und

(b) für sämtliche Obliegenheiten, die den Unterauftragsverarbeitern übertragenwurden, und für sämtliches Tun und Unterlassen ihrer Unterauftragsverarbeiter vollumfänglich haften.

11.4 **Möglichkeit des Widerspruch gegen Änderungen bei der Unterauftragsvergabe.**

(a) Wenn während der Laufzeit ein neuer Dritt-Unterauftragsverarbeiter beauftragt wird, wird Google den Kunden mindestens 30 Tage bevor dieser neue Dritt-Unterauftragsverarbeiter mit der Verarbeitung von personenbezogenen Daten des Kunden betraut wird durch Zusendung einer E-Mail an die E-Mail-Adresse für Benachrichtigungen über die Beauftragung informieren (einschließlich des Namens und Standorts des jeweiligen Unterauftragsverarbeiters und der Tätigkeiten, die dieser ausführen wird).

(b) Der Kunde kann dem Einsatz eines neuen Dritt-Unterauftragsverarbeiters widersprechen, indem er die Vereinbarung sofort schriftlich kündigt; dies hat innerhalb von 90 Tagen nach Erhalt der Benachrichtigung über die Beauftragung des jeweiligen Unterauftragsverarbeiters, wie in Ziffer 11.4(a) beschrieben, zu erfolgen. Dieses Kündigungsrecht ist der einzige und ausschließliche Rechtsbehelf des Kunden, wenn er mit dem Einsatz eines neuen Dritt-Unterauftragsverarbeiters nicht einverstanden ist.

12. Kontaktaufnahme mit Google; Aufzeichnungen über die Verarbeitung

12.1 **Kontaktaufnahme mit Google.** Der Kunde kann Google über die Möglichkeiten, die unter privacy.google.com/businesses/processorsupport aufgeführt sind bzw. über andere von Google ggf. dafür bereitgestellte Möglichkeiten kontaktieren, um seine Rechte unter diesen Datenverarbeitungsbedingungen auszuüben.

12.2 **Googles Aufzeichnungen über die Datenverarbeitung.** Der Kunde nimmt zur Kenntnis, dass Google unter der DSGVO verpflichtet ist: (a) Aufzeichnungen über bestimmte Informationen anzufertigen und vorzuhalten, darunter den Namen und Kontaktdaten von jedem Verarbeiter und/oder Verantwortlichen in deren Auftrag Google handelt und (falls zutreffend) Informationen über den Vertretungsberechtigten vor Ort und den Datenschutzbeauftragten; und (b) diese Informationen der jeweiligen Aufsichtsbehörde zugänglich zu machen. Dementsprechend ist der Kunde verpflichtet, diese Informationen auf Aufforderung und soweit für den Kunden anwendbar, Google über die Benutzeroberfläche der Auftragsverarbeiterdienste oder über andere von Google ggf. dafür bereitgestellte Möglichkeiten zu übermitteln und die Benutzeroberfläche oder ggf. eine andere dafür bereitgestellte Möglichkeit zu nutzen, um sicherzustellen, dass diese Angaben stets korrekt und aktuell sind.

13. Haftung

Wenn die Vereinbarung den Gesetzen:

(a) eines Bundesstaates der Vereinigten Staaten von Amerika unterliegt, dann gilt, ungeachtet einer anderen Regelung in der

Vereinbarung, für die Gesamthaftung der jeweiligen Partei unter oder in Verbindung mit diesen Datenschutzbestimmungen der summenmäßige Haftungshöchstbetrag, auf den die Haftung der jeweiligen Partei gemäß der Vereinbarung begrenzt ist (zur Klarstellung, jeglicher Ausschluss von Haftungsfreistellungsansprüchen auf Grundlage der Haftungsbegrenzungsregelung der Vereinbarung gilt nicht für Haftungsfreistellungsansprüche unter der Vereinbarung in Bezug auf die Datenschutzvorschriften) oder

(b) eines anderen Landes als dem eines Bundesstaates der Vereinigten Staaten von Amerika unterliegt, richtet sich die Haftung unter oder gemäß diesen Datenverarbeitungsbedingungen nach den Haftungsbeschränkungen und -ausschlüssen der Vereinbarung.

14. Geltung dieser Datenverarbeitungsbedingungen

Im Fall eines Widerspruchs oder einer Abweichung zwischen diesen Datenverarbeitungsbedingungen und der übrigen Vereinbarung haben die Regelungen dieser Datenverarbeitungsbedingungen Vorrang. Mit Ausnahme der Änderungen durch diese Datenverarbeitungsbedingungen bleibt die Vereinbarung ansonsten weiterhin in vollem Umfang wirksam und in Kraft.

15. Änderungen dieser Datenverarbeitungsbedingungen

15.1 **Änderungen der URLs.** Google kann gelegentlich URLs, auf die in diesen Datenverarbeitungsbedingungen Bezug genommen wird, und die Inhalte auf solchen URLs ändern. Google ist aber nur berechtigt, die Auflistung der möglichen Auftragsverarbeiterdienste unter privacy.google.com/businesses/adsservices zu ändern:

(a) um einer Umbenennung eines Dienstes Rechnung zu tragen;

(b) um einen neuen Dienst hinzuzufügen; oder

(c) um einen Dienst zu entfernen, jedoch nur für den Fall, dass (i) sämtliche Verträge über die Erbringung dieses Dienstes beendet wurden oder (ii) Google dazu die Zustimmung des Kunden vorliegt.

15.2 **Änderungen der Datenverarbeitungsbedingungen.** Google kann diese Datenverarbeitungsbedingungen ändern, wenn eine solche Änderung:

(a) ausdrücklich durch die vorliegenden Datenverarbeitungsbedingungen erlaubt ist, einschließlich gemäß Ziffer 15.1 (Änderungen der URLs);

(b) einer Änderung des Unternehmensnamens oder eine Änderung der Rechtsform Rechnung trägt;

(c) erforderlich ist, um anwendbarem Recht, anwendbaren Vorschriften, einer Gerichtsentscheidung oder einer Vorgabe einer staatlichen Regulierungs- oder Aufsichtsbehörde zu entsprechen; oder

(d) (i) nicht zu einer Verschlechterung der Gesamtsicherheit der Auftragsverarbeiterdienste führt, (ii) den Anwendungsbereich dieser Datenverarbeitungsbedingungen nicht ausweitet oder Beschränkungen wie Ziffer 5.3 (Befolgung der Weisungen durch Google) beschrieben hinsichtlich der Verarbeitung personenbezogener Daten des Kunden durch Google nicht aufhebt, und (iii) auch sonst zu keinen erheblichen nachteiligen Auswirkungen auf die Rechte des Kunden unter diesen Datenverarbeitungsbedingungen führt (dies wird auf angemessene Weise durch Google bestimmt).

15.3 **Benachrichtigung über Änderungen.** Wenn Google beabsichtigt, diese Datenverarbeitungsbedingungen gemäß Ziffer 15.2(c) oder (d) zu ändern, wird Google dies dem Kunden mindestens 30 Tage vor Wirksamwerden der Änderung im Voraus (oder innerhalb einer kürzeren Frist, falls dies nach anwendbarem Recht, anwendbaren Vorschriften, aufgrund einer Gerichtsentscheidung oder eine Vorgabe einer staatlichen Regulierungs- oder Aufsichtsbehörde erforderlich ist) mitteilen durch: (a) die Übermittlung einer E-Mail an die E-Mail-Adresse für Benachrichtigungen oder (b) durch Benachrichtigung über die Benutzeroberfläche des Auftragsverarbeiterdienstes. Wenn der Kunde einer Änderung widersprechen möchte, kann der Kunde die Vereinbarung durch schriftliche Mitteilung gegenüber Google innerhalb von 90 Tagen nach Erhalt der Benachrichtigung über die Änderung durch Google kündigen.

Anhang 1: Gegenstand und Details zur Datenverarbeitung

Gegenstand

Bereitstellung von Auftragsverarbeiterdiensten und damit in Zusammenhang stehendem technischen Supportleistungen für den Kunden durch Google.

Dauer der Datenverarbeitung

Während der Vertragslaufzeit und zusätzlich während eines Zeitraums zwischen dem Ende der Vertragslaufzeit und bis zur Löschung aller personenbezogenen Daten des Kunden durch Google in Übereinstimmung mit den vorliegenden Datenverarbeitungsbedingungen.

Art und Zweck der Datenverarbeitung

Google verarbeitet personenbezogene Daten des Kunden zum Zweck, dem Kunden die Auftragsverarbeiterdienste bereitzustellen und den damit im Zusammenhang stehenden technischen Support in Übereinstimmung mit diesen Datenverarbeitungsbedingungen zu erbringen. Die Datenverarbeitung durch Google schließt, in Abhängigkeit davon, ob es auf den jeweiligen Auftragsverarbeiterdienst und die in Ziffer 5.2 (Weisungen des Kunden) beschriebenen Weisungen zutrifft, das Erheben, Erfassen, Organisieren, Ordnen, Verändern, Auslesen, Verwenden, Offenlegen, Verknüpfen, Löschen oder Vernichten mit ein.

Arten personenbezogener Daten

Personenbezogene Daten des Kunden können solche Arten personenbezogener Daten umfassen, die unter privacy.google.com/businesses/adsservices beschrieben sind.

Kategorien betroffener Personen

Personenbezogene Daten des Kunden betreffen die folgenden Kategorien von betroffenen Personen:

- betroffene Personen, über die Google im Rahmen der Erbringung der Auftragsverarbeiterdienste personenbezogene Daten erhebt; und/oder
- betroffene Personen, von denen personenbezogene Daten auf Veranlassung oder im Auftrag des Kunden im Zusammenhang mit den Auftragsverarbeiterdiensten an Google übermittelt werden.

Je nach Art des jeweiligen Auftragsverarbeiterdienstes können betroffene Personen folgende Einzelpersonen umfassen: Personen, (a) an die Online-Werbung gerichtet wurde oder werden wird, (b) die bestimmte Webseiten oder Applikationen aufgerufen haben, für die Google die Auftragsverarbeiterdienste bereitstellt und/oder (c) die Kunden oder Nutzer von Produkten oder Diensten des Kunden sind.

Anhang 2: Sicherheitsmaßnahmen

Google verpflichtet sich, ab dem Wirksamkeitsdatum die Sicherheitsmaßnahmen, die in diesem Anhang 2 enthalten sind, zu implementieren und aufrechtzuerhalten. Google kann diese Sicherheitsmaßnahmen gelegentlich aktualisieren oder ändern, vorausgesetzt dass solche Aktualisierungen und Änderungen nicht zu einer Verschlechterung der allgemeinen Sicherheit der Auftragsverarbeiterdienste führen.

1. Sicherheit der Rechenzentren und des Netzwerks

(a) **Rechenzentren.**

Infrastruktur. Google betreibt geographisch verteilte Rechenzentren. Google speichert alle Produktionsdaten in physisch

gesicherten Rechenzentren.

Redundanz. Die Infrastruktursysteme wurden entwickelt, um Single Points of Failure (zentrale Schwachpunkte) zu beseitigen und um die Auswirkungen der zu erwartenden Umgebungsrisiken zu minimieren. Duale Stromkreise, Switches, Netzwerke oder andere erforderliche Geräte helfen, diese Redundanz zu erreichen. Die Auftragsverarbeiterdienste sind so konzipiert, dass Google bestimmte vorbeugende und fehlerbehebende Instandhaltungsmaßnahmen ohne Unterbrechung durchführen kann. Es gibt für sämtliche Anlagen und Einrichtungen dokumentierte, vorbeugende Instandhaltungsverfahren, die ausführlich den Prozess und die Häufigkeit der Durchführung in Übereinstimmung mit den Herstellervorgaben oder internen Vorgaben beschreiben. Vorbeugende und fehlerbehebende Instandhaltungsmaßnahmen der Anlagen im Rechenzentrum werden über einen Standardprozess gemäß dokumentierten Verfahren geplant.

Energie. Die Energiesysteme der Rechenzentren sind so entworfen, dass sie redundant sein sollen und gewartet werden können, ohne dass dies einen Einfluss auf den Dauerbetrieb (24 Stunden am Tag und 7 Tage die Woche) hat. In den meisten Fällen steht sowohl eine primäre als auch eine alternative Energiequelle, jeweils mit gleicher Kapazität, für kritische Infrastruktur-Komponenten in den Rechenzentren zur Verfügung. Reserveleistung wird durch verschiedene Mechanismen wie etwa unterbrechungsfreie Stromversorgungs-Batterien (USV), die beständig zuverlässigen Leistungsschutz bei Spannungsabfällen, Stromausfällen, Überspannung, Unterspannung und außerhalb der Toleranzwerte liegende Frequenzbedingungen durch den Energieversorger bieten. Falls die Stromversorgung des Energieversorgers unterbrochen wird, ist die Ersatzversorgung so entworfen, dass die Rechenzentren übergangsweise bei voller Last Energie für bis zu 10 Minuten erhalten sollen bis die Diesel-Generatoren die Versorgung übernehmen. Die Diesel-Generatoren sind darauf ausgelegt, automatisch innerhalb von Sekunden anzuspringen und genug Notstrom bereitzustellen, um das Rechenzentrum bei voller Leistung in der Regel für einen Zeitraum von mehreren Tagen zu betreiben.

Server-Betriebssysteme. Google-Server verwenden gehärtete Betriebssysteme, die für die spezifischen Anforderungen des Betriebs angepasst sind. Daten werden unter Verwendung von proprietären Algorithmen gespeichert, um die Datensicherheit und Redundanz zu steigern. Google setzt einen Code-Überprüfungsprozess ein, um die Sicherheit des Programmiercodes, der für die Bereitstellung der Auftragsverarbeiterdienste verwendet wird, zu erhöhen und die Sicherheits-Produkte in Produktionsumgebungen zu verbessern.

Aufrechterhaltung des Betriebs. Google repliziert Daten über mehrere Systeme, um dazu beizutragen, die Daten vor zufälliger Zerstörung oder Verlust zu schützen. Google hat Pläne, um den Betrieb aufrecht zu erhalten, und Notfallwiederherstellungsprogramme entworfen. Google entwickelt diese weiter und testet sie.

(b) **Netzwerke und Übertragung.**

Datenübertragung. Rechenzentren sind in der Regel über Hochgeschwindigkeitsdirektverbindungen (High-Speed-Private-Links) verbunden, um eine sichere und schnelle Datenübertragung zwischen den Rechenzentren bereit zu stellen. Dieses Verfahren ist so entwickelt worden, dass ein unberechtigtes Auslesen, Kopieren, Verändern oder Entfernen von Daten während der elektronischen Übertragung oder des Transports oder bei der Speicherung auf Datenträgern verhindert werden soll. Google überträgt Daten mittels Internet-Standard-Protokollen.

Externe Angriffsfläche. Google unterhält mehrere Schichten von Netzwerkgeräten und Einbruchserkennungssystemen, um die externe Angriffsfläche zu sichern. Google zieht potenzielle Angriffsvektoren in Betracht und integriert angemessene, speziell entwickelte Technologien in von außen erreichbare Systeme.

Einbruchserkennung. Die Maßnahmen zur Einbruchserkennung zielen darauf ab, Einblicke in laufende Angriffsaktivitäten zu ermöglichen und angemessene Informationen zu liefern, um auf Vorfälle zu reagieren. Googles Maßnahmen zur Erkennung von Einbrüchen beinhalten:

1. die strenge Überwachung der Größe und des Aufbaus von Googles Angriffsfläche durch vorbeugende Maßnahmen,
2. den Einsatz von intelligenten Entdeckungskontrollmaßnahmen an Datenerfassungspunkten und
3. den Einsatz von Technologien, die bestimmte gefährliche Situationen automatisch abstellen.

Reaktion auf Zwischenfälle. Google überwacht eine Vielzahl von Kommunikationskanälen auf Sicherheitsvorfälle. Googles Sicherheitspersonal wird umgehend auf bekannt gewordene Vorfälle reagieren.

Verschlüsselungstechnologien. Google stellt HTTPS-Verschlüsselung (auch SSL- oder TLS-Verbindung genannt) zur Verfügung. Google Server unterstützen einen auf Basis elliptischer Kurven stattfindenden Ephemeral Diffie-Hellman Austausch von RSA und ECDSA signierten Schlüsseln. Diese auf ‚perfekt vorwärts' gerichtete Geheimhaltungsmethoden (perfect forward secrecy (PFS)) helfen, den Datenverkehr zu schützen und den Einfluss eines kompromittierten Schlüssels oder einer Durchbrechung der Verschlüsselung (cryptographic breakthrough) zu minimieren.

2. Zugangs- und Zutrittskontrollen

(a) **Zutrittskontrolle.**

Vor-Ort-Überwachung der Rechenzentren. Googles Rechenzentren verfügen über einen Vor-Ort-Sicherheitsdienst, der für sämtliche physischen Sicherheitsmaßnahmen des Rechenzentrums 24 Stunden am Tag, 7 Tage die Woche verantwortlich ist. Das Sicherheitspersonal vor Ort kontrolliert Überwachungskameras und sämtliche Alarmanlagen. Das Sicherheitspersonal unternimmt vor Ort regelmäßig Kontrollgänge innerhalb und außerhalb des Rechenzentrums.

Verfahren für den Zutritt zu Rechenzentren. Google unterhält Zutrittskontrollverfahren für den physischen Zugang zu Rechenzentren. Die Rechenzentren sind in Einrichtungen untergebracht, die für den Zugang elektronische Schlüsselkarten erfordern, wobei Alarmanlagen mit dem Sicherheitsdienst vor Ort verbunden sind. Jeder, der ein Rechenzentrum betreten möchte, muss sich ausweisen und einen Nachweis seiner Identität gegenüber dem Sicherheitspersonal vorlegen. Nur berechtigten Angestellten, Auftragnehmern und Besuchern wird Zugang zu den Rechenzentren gewährt. Nur berechtigten Mitarbeitern und Auftragnehmern ist es erlaubt, Zutrittsrechte per elektronischer Schlüsselkarte zu diesen Einrichtungen zu beantragen. Anträge für den Zugang zu Rechenzentren mit einer elektronischen Schlüsselkarte müssen im Voraus und schriftlich beantragt werden und erfordern die Zustimmung des Vorgesetzten des Antragstellers sowie des Leiters des Rechenzentrums. Jeder andere, der vorübergehend Zugang zum Rechenzentrum benötigt, muss (i) im Voraus die Zustimmung der Manager des Rechenzentrums, dessen Besuch beabsichtigt ist, einholen; (ii) sich beim Sicherheitspersonal vor Ort anmelden; und (iii) einen Nachweis einer Zutrittsgenehmigung vorlegen, der die Person als autorisiert identifiziert.

Vor-Ort Sicherheitseinrichtungen der Rechenzentren. Googles Rechenzentren verfügen über ein elektronisches Schlüsselkarten- und biometrisches Zutrittskontrollsystem, das mit einem Alarm-System verbunden ist. Das Zutrittskontrollsystem überwacht und protokolliert den Einsatz der Schlüsselkarte jeder einzelnen Person und wann diese Außentüren, Versand- oder Wareneingangsbereiche sowie andere kritische Bereiche betreten. Unberechtigte Aktivitäten und fehlgeschlagene Zutrittsversuche werden vom Zutrittskontrollsystem protokolliert und, soweit angemessen, untersucht. Der berechtigte Zutritt während der Geschäftszeiten und innerhalb des gesamten Rechenzentrums ist auf bestimmte Zonen beschränkt, die von dem jeweiligen beruflichen Aufgabenbereich abhängen. Die Brandschutztüren sind alarmgesichert. Überwachungskameras sind sowohl innerhalb als auch außerhalb der Rechenzentren in Betrieb. Die Positionierung der Kameras wurde so geplant, dass sie strategische Bereiche, wie unter anderem den Außenbereich, Eingangstüren der Rechenzentrumsgebäude und Versand- und Wareneingangsbereiche, überwachen sollen. Das Sicherheitspersonal vor Ort kontrolliert die Bildschirme der Überwachungskameras sowie die Aufnahme- und Steuerungseinrichtungen. Gesicherte Leitungen verbinden die Überwachungskameratechnik im gesamten Rechenzentrum. Die Kameras zeichnen vor Ort 24 Stunden am Tag, 7 Tage die Woche auf. Die Aufnahmen werden mindestens für 7 Tage in Abhängigkeit von den jeweiligen Aktivitäten aufbewahrt.

(b) **Zugriffskontrolle.**

Sicherheitspersonal für die Infrastruktur. Google hat eine Sicherheitsrichtlinie für ihr Personal erlassen und erhält diese aufrecht. Google verlangt von ihren Mitarbeitern die Teilnahme an einem Sicherheitstraining als Teil eines Schulungsprogramms. Googles Personal für die Sicherheit der Infrastruktur ist für die laufende Überwachung der Sicherheit von Googles Infrastruktur, die Überprüfung der Auftragsverarbeiterdienste und die Reaktion auf Sicherheitsvorfälle verantwortlich.

Zugriffskontrolle und Rechteverwaltung. Administratoren und Endnutzer müssen sich über ein zentrales Authentifizierungssystem oder über ein Single Sign-On-System authentifizieren, um die Auftragsverarbeiterdienste zu nutzen.

Interne Datenzugriffsprozesse und Richtlinien – Zugriffsrichtlinien. Googles interne Datenzugriffsprozesse und Richtlinien sind so gestaltet, dass Zugriffe auf Systeme, die genutzt werden, um personenbezogene Daten zu verarbeiten, durch unberechtigte Personen und/oder Systeme verhindert werden soll. Google ist bestrebt, die Systeme so zu gestalten, dass: (i) nur berechtigten Personen Zugang zu den Daten gewährt wird, für die sie zugriffsberechtigt sind; und (ii) sichergestellt ist, dass personenbezogene Daten ohne entsprechende Berechtigung während ihrer Verarbeitung, Nutzung und nach ihrer Speicherung nicht gelesen, kopiert, verändert oder gelöscht werden können. Die Systeme sind darauf ausgelegt, dass sie möglichst jeden unberechtigten Zugriff erkennen sollen. Google setzt ein zentralisiertes Zugriffsverwaltungssystem zur Kontrolle von Mitarbeiterzugriffen auf Produktionsserver ein und gewährt nur einem beschränkten Kreis von berechtigten Mitarbeiter Zugriff. LDAP, Kerberos und ein proprietäres System, das SSH-Zertifikate einsetzt, sind so angelegt, dass Google über sichere und flexible Zugriffsmechanismen verfügen soll. Diese Mechanismen sind so konzipiert, dass nur mit entsprechender Berechtigung Zugriffe auf Site-Hosts, Log-Dateien, Daten und Konfigurationsinformationen gewährt werden sollen. Google verlangt die Benutzung singulärer Benutzer-IDs und sicherer Passwörter; die Bestätigung in zwei Schritten (two factor authentication) und sorgfältig überwachte Zugriffslisten, um die Möglichkeiten einer unberechtigten Nutzung des Accounts 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 Stelle, um berechtigte Aufgaben auszuführen und einer Need-to-Know-Basis. Die Gewährung oder Änderung von Zugriffsrechten muss außerdem auch in

Übereinstimmung mit Googles internen Datenzugriffsrichtlinien und -schulungen stehen. Zugriffsberechtigungen werden über workflowbasierte Werkzeuge verwaltet, die Audit-Datensätze über alle Änderungen erstellen. Der Zugriff auf Systeme wird protokolliert, um einen Audittrail zur Rechenschaftsablegung zu erstellen. Wo Passwörter zur Authentifizierung eingesetzt werden (z.B. zum Login an Arbeitsplatzrechnern), sind Passwortrichtlinien eingerichtet worden, die mindestens dem Industriestandard entsprechen. Diese Vorgaben umfassen Einschränkungen zur Wiederverwendung von Passwörtern und eine hinreichende Passwortstärke.

3. Daten

(a) **Datenspeicherung, Isolation und Authentifizierung.**

Google speichert die Daten in einer mandantenfähigen Umgebung (Multi-Tenant Umgebung) auf Servern, die im Eigentum von Google stehen. Die Daten, die Datenbanken der Auftragsverarbeiterdienste und die Architektur des Dateiverwaltungssystems werden in mehreren geographisch verteilten Rechenzentren repliziert. Google isoliert die individuellen Daten jedes einzelnen Kunden logisch voneinander. Für alle Auftragsverarbeiterdienste wird übergreifend ein zentrales Authentifizierungssystem genutzt, um die allgemeine Datensicherheit zu erhöhen.

(b) **Stilllegung und Richtlinien zur Zerstörung von Festplatten.**

Falls bei bestimmten Festplatten, die Daten enthalten, eine verminderte Leistungsfähigkeit, Fehler oder Hardwareausfällen festgestellt wird, werden die betroffenen Festplatten stillgelegt (**„stillgelegte Festplatte“**). Jede stillgelegte Festplatte durchläuft eine Serie von Zerstörungsprozessen (**„Richtlinien zur Zerstörung von Daten“**) bevor sie Googles Betriebsgelände entweder zur Wiederverwendung oder zur Zerstörung verlässt. Stillgelegte Festplatten werden zunächst in einem mehrstufigen Prozess gelöscht. Die vollständige Löschung muss daraufhin von mindestens zwei unabhängigen Prüfern bestätigt werden. Die Löschergebnisse werden anhand der Seriennummer der stillgelegten Festplatte zur Nachverfolgung gespeichert. Abschließend wird die gelöschte stillgelegte Festplatte im Inventar zur Wiederverwendung freigegeben. Falls eine stillgelegte Festplatte aufgrund eines Hardwareversagens nicht gelöscht werden kann, wird sie sicher verwahrt bis sie zerstört werden kann. Jede Einrichtung wird regelmäßig auditiert, um zu überwachen, dass die Richtlinien zur Zerstörung von Daten eingehalten werden.

4. Personalsicherheit.

Das Personal von Google ist verpflichtet, sich gemäß den Unternehmensrichtlinien über Vertraulichkeit, Unternehmensethik und sachgemäßen Gebrauch sowie gemäß beruflichen Standards zu verhalten. Google führt im angemessenen Umfang Hintergrundsüberprüfungen durch, soweit dies im Einklang mit geltendem Recht, insbesondere mit anwendbarem nationalen Arbeitsrecht und verpflichtend geltenden anderen Gesetzen steht.

Das Personal ist verpflichtet, eine Vertraulichkeitsvereinbarung zu unterzeichnen und deren Erhalt und die Einhaltung von Googles Vertraulichkeits- und Datenschutzbestimmungen zu bestätigen. Das Personal erhält Sicherheitsschulungen. Das Personal, das Kundendaten handhabt, muss in Abhängigkeit vom jeweiligen Aufgabenbereich zusätzliche Voraussetzungen erfüllen. Googles Personal wird keine personenbezogenen Daten des Kunden verarbeiten, ohne dazu berechtigt zu sein.

5. Sicherheit bei Unterauftragsverarbeitern

Bevor Unterauftragsverarbeiter eingesetzt werden, führt Google zunächst eine Auditierung der Sicherheits- und Datenschutzpraxis des Unterauftragsverarbeiters durch, um sicherzustellen, dass ein Sicherheits- und Datenschutzniveau besteht, das im angemessenen Verhältnis zum Datenzugriff und dem Umfang der beauftragten Dienstleistungen steht. Sobald Google die vom Unterauftragsverarbeiter dargelegten Risiken einschätzen kann, ist der Unterauftragsverarbeiter stets vorbehaltlich der in Ziffer 11.3 (Anforderungen für die Beauftragung von Unterauftragsverarbeitern) dieser Datenverarbeitungsbedingungen festgelegten Anforderungen verpflichtet, angemessene Sicherheits-, Vertraulichkeits- und Datenschutzvereinbarungen abzuschließen.

Auftragsdatenverarbeitungsbedingungen für Google Werbeprodukte (Google Ads Data Processing Terms), Version 1.3

31. Oktober 2019

Vorherige Versionen

- 12. Oktober 2017