Diese Übersetzung dient ausschließlich Informationszwecken und spiegelt die ursprüngliche englische Bedeutung nicht unbedingt genau wider. Die Bedeutungen der hierin enthaltenen Bedingungen, Bestimmungen und Zusicherungen unterliegen ihren jeweiligen Definitionen und Auslegungen in der englischen Sprache. Im Falle von Diskrepanzen oder Widersprüchen zwischen der englischen Version dieses Texts und Übersetzungen gilt die englische Version.

NACHTRAG ZUR DATENVERARBEITUNG VON CLOUDFLARE

Cloudflare, Inc. („**Cloudflare**“) und der Vertragspartner, der diesen Bestimmungen zustimmt (der „**Kunde**“) haben einen Abonnementvertrag für Unternehmen, ein *Self-Serve Subscription Agreement* oder eine andere schriftliche oder elektronische Vereinbarung über die von Cloudflare bereitgestellten Dienste abgeschlossen (der „**Hauptvertrag**“). Dieser Nachtrag zur Datenverarbeitung zusammen mit seinen Anhängen (der „**Nachtrag**“) bildet einen Teil des Hauptvertrags.

Dieser Nachtrag ersetzt ab dem Datum, an dem der Kunde diesen Nachtrag unterzeichnet oder die Parteien ihn anderweitig abschließen („**Nachtrag-Gültigkeitsdatum**“), alle zuvor anwendbaren Bestimmungen in Bezug auf seinen Gegenstand (einschließlich aller Datenverarbeitungsergänzungen, -vereinbarungen oder -zusätze in Bezug auf die Dienste).

Wenn Sie diesen Nachtrag im Namen eines Kunden akzeptieren, sichern Sie zu: (a) dass Sie über die rechtliche Befugnis verfügen, den Kunden an diesen Nachtrag zu binden; (b) dass Sie diesen Nachtrag gelesen und verstanden haben; und (c) dass Sie im Namen des Kunden diesem Nachtrag zustimmen. Wenn Sie nicht über die rechtliche Befugnis verfügen, den Kunden an diesen Nachtrag zu binden, dürfen Sie diesen Nachtrag nicht akzeptieren.

DATENVERARBEITUNGSBESTIMMUNGEN

Dieser Nachtrag findet Anwendung, wenn Cloudflare als Auftragsverarbeiter (oder Unterauftragsverarbeiter, falls zutreffend) personenbezogene Daten im Auftrag des Kunden verarbeitet, um die Dienste zur Verfügung zu stellen, und diese personenbezogenen Daten den Anwendbaren Datenschutzgesetzen (wie unten definiert) unterliegen.

Die Parteien haben diesen Nachtrag geschlossen, um sicherzustellen, dass geeignete Garantien bestehen, um diese personenbezogenen Daten in Einklang mit den Anwendbaren Datenschutzgesetzen zu schützen. Dementsprechend erklärt Cloudflare, die folgenden Bestimmungen in Bezug auf die von Cloudflare als Auftragsverarbeiter (oder Unterauftragsverarbeiter, falls zutreffend) im Auftrag des Kunden verarbeiteten personenbezogenen Daten einzuhalten.

1. **Definitionen**

1.1 In diesem Nachtrag werden die folgenden Begriffe verwendet:

a) „**Land mit angemessenem Schutzniveau**“ bezeichnet ein Land oder Gebiet, das in Einklang mit den Europäischen Datenschutzgesetzen als Land anerkannt ist, welches ein angemessenes Schutzniveau für personenbezogene Daten bereitstellt.

b) „**Verbundenes Unternehmen**“ bezeichnet in Bezug auf eine Partei jedes Unternehmen, das direkt oder indirekt diese Partei kontrolliert, von ihr kontrolliert wird oder sich mit ihr unter gemeinsamer Kontrolle befindet (jedoch nur so lange eine solche Kontrolle besteht).

c) „**Anwendbare Datenschutzgesetze**“ bezeichnet alle Gesetze und Vorschriften, die für die Verarbeitung personenbezogener Daten im Rahmen des Hauptvertrags gelten, einschließlich der Europäischen Datenschutzgesetze und der Datenschutzgesetze der Vereinigten Staaten.

d) „**Cloudflare-Unternehmensgruppe**“ bezeichnet Cloudflare und alle seine Verbundenen Unternehmen.

e) „**Verantwortlicher**“ bezeichnet die Einheit, die den Zweck und die Mittel der Verarbeitung personenbezogener Daten festlegt und umfasst auch "Verantwortliche" oder gleichbedeutende Begriffe, wie in den Anwendbaren Datenschutzgesetzen definiert.

f) „**Unternehmensgruppe des Kunden**“ bezeichnet den Kunden und alle seine Verbundenen Unternehmen.

g) „**Europäische Datenschutzgesetze**“ bezeichnet alle Gesetze und Verordnungen der Europäischen Union, des Europäischen Wirtschaftsraums, ihrer Mitgliedsstaaten, der Schweiz und des Vereinigten Königreichs, die auf die Verarbeitung personenbezogener Daten im Rahmen des Hauptvertrags Anwendung finden (einschließlich, soweit zutreffend, (i) der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) (die „**EU-DSGVO**“); (ii) die EU-DSGVO in der Form, in der sie durch Abschnitt 3 des EU-Austrittsgesetzes des Vereinigten Königreichs (*European Union (Withdrawal) Act*) von 2018 in britisches Recht übertragen wurde und den britischen *Data Protection Act* von 2018 (die „**UK-DSGVO**“); (iii) des Schweizer Datenschutzgesetzes vom 19. Juni 1992 (das „**Schweizer Datenschutzgesetz**“); (iv) der e-Privacy-Richtlinie der EU (Richtlinie 2002/58/EG); und (iv) sämtlicher anwendbarer nationaler Datenschutzgesetze, die gemäß oder infolge von (i), (ii), (iii) oder (iv) erlassen wurden oder gemeinsam mit diesen Anwendung finden.

h) „**Personenbezogene Daten**“ bezeichnet alle Daten, die in den Anwendbaren Datenschutzgesetzen als „*personenbezogene Daten*“, „*personenbezogene Informationen*“ oder „*persönlich identifizierbare Informationen*“ (oder gleichwertige Begriffe) definiert sind.

i) Die Begriffe „**Verarbeitung**“, „**betroffene Person**“ und „**Aufsichtsbehörde**“ haben die Bedeutungen, wie in den Europäischen Datenschutzgesetzen definiert.

j) „**Auftragsverarbeiter**“ bezeichnet ein Unternehmen, das personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet, einschließlich eines Unternehmens, dem gegenüber ein anderes Unternehmen die personenbezogenen Daten einer natürlichen Person für geschäftliche Zwecke im Rahmen eines Vertrags offenlegt, der das Unternehmen, welches die Daten erhält, dazu verpflichtet, personenbezogene Daten nur für den Zweck der Bereitstellung der Dienste zu speichern, zu nutzen oder weiterzugeben, und der Begriff umfasst auch „Auftragsverarbeiter“, „Dienstleister“ oder gleichwertige Begriffe, die in den Anwendbaren Datenschutzgesetzen definiert sind.

k) „**Dienste**“ bezeichnet alle Cloud-basierten Lösungen, die von Cloudflare oder seinen autorisierten Partnern angeboten, vermarktet oder verkauft werden und die Performance, Sicherheit und Verfügbarkeit von Internetwebsites, Anwendungen und Netzwerken verbessern sollen. Darunter fallen außerdem jegliche Softwareprodukte, Software Development Kits und Anwendungsprogrammierschnittstellen („**APIs**“), die im Zusammenhang mit dem Vorgenannten bereitgestellt werden.

l) „**EU-SCC**“ bezeichnet die dem Durchführungsbeschluss der Europäischen Kommission 2021/914 vom 4. Juni 2021 beigefügten Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates.

m) „**Beschränkte Übermittlung**“ bezeichnet: (i) soweit die EU-DSGVO oder das Schweizer Datenschutzgesetz Anwendung findet, eine Übermittlung personenbezogener Daten aus dem Europäischen Wirtschaftsraum oder der Schweiz (soweit zutreffend) in ein Land außerhalb des Europäischen Wirtschaftsraums oder der Schweiz (soweit zutreffend), das nicht Gegenstand eines Angemessenheitsbeschlusses der Europäischen Kommission oder des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten der Schweiz (soweit zutreffend) ist; und (ii) soweit die UK-DSGVO Anwendung findet, eine Übermittlung personenbezogener Daten aus dem Vereinigten Königreich in ein anderes Land, die nicht auf den Angemessenheitsbestimmungen gemäß Abschnitt 17A des britischen *Data Protection Act* von 2018 beruht.

n) „**UK Addendum**“ bezeichnet das *International Data Transfer Addendum* (Version B1.0), das vom *Information Commissioner's Office* gemäß s.119(A) der UK-DSGVO erlassen wurde, in seiner jeweils aktuellen Version.

o) „**Datenschutzgesetze der Vereinigten Staaten**“ bezeichnet alle Gesetze und Verordnungen der Vereinigten Staaten, die auf die Verarbeitung personenbezogener Daten gemäß dem Hauptvertrag anwendbar sind, einschließlich (a) des *California Consumer Privacy Act* von 2018, in seiner durch den *California Privacy Rights Act* von 2020 geänderten Form (Cal. Civ. Code § 1798.100 - 1798.199, 2022) und der diesen umsetzenden Verordnungen (gemeinsam: der „CCPA“), (b) des *Consumer Data Protection Act* von Virginia, sobald in Kraft getreten, (c) des *Privacy Act* von Colorado und der diesen umsetzenden Verordnungen, sobald in Kraft getreten, (d) des *Consumer Privacy Act* von Utah, sobald in Kraft getreten und (e) des *SB6, An Act Concerning Personal Data Privacy and Online Monitoring* von Connecticut, sobald in Kraft getreten.

1.2 Ein Unternehmen „**kontrolliert**“ ein anderes Unternehmen, wenn es: (a) eine Mehrheit der Stimmrechtsanteile an ihm besitzt; (b) ein Mitglied oder Anteilhaber des anderen Unternehmens ist und das Recht besitzt, eine Mehrheit der Mitglieder seines Vorstands oder eines gleichwertigen Verwaltungsgremiums zu entfernen; (c) ein Mitglied oder Anteilhaber des anderen Unternehmens ist und allein oder im Rahmen einer Vereinbarung mit anderen Anteilhabern oder Mitgliedern eine Mehrheit der Stimmrechtsanteile an ihm kontrolliert; oder (d) gemäß den Gründungsdokumenten des anderen Unternehmens oder gemäß einem Vertrag das Recht besitzt, einen maßgeblichen Einfluss über das andere Unternehmen auszuüben; und zwei Unternehmen gelten als unter „ **gemeinsamer Kontrolle**“, wenn eines davon das andere (direkt oder indirekt) kontrolliert oder wenn beide (direkt oder indirekt) vom selben Unternehmen kontrolliert werden.

1.3 Für die Zwecke dieses Nachtrags bezeichnet „bereitstellen“ oder „Bereitstellung“ der Dienste das Erbringen der Dienste, wie in dem Hauptvertrag definiert.

2. Rollen der Parteien

2.1 Die Art der gemäß dieses Nachtrags verarbeiteten personenbezogenen Daten und der Gegenstand, die Dauer, die Art und der Zweck der Verarbeitung sowie die Kategorien betroffener Personen sind in Anhang 1 beschrieben.

2.2 Jede Partei sichert in Bezug auf personenbezogene Daten zu, dass sie die Anwendbaren Datenschutzgesetze einhalten und das danach verlangte Datenschutzniveau bieten wird. Zwischen den Parteien trägt der Kunde die alleinige Verantwortung für die Richtigkeit, Qualität und Rechtmäßigkeit der personenbezogenen Daten sowie für die Mittel, mit denen der Kunde die personenbezogenen Daten erhoben hat.

2.3 Hinsichtlich der Rechte und Pflichten der Parteien im Rahmen dieses Nachtrags bezüglich personenbezogener Daten bestätigen und vereinbaren die Parteien, dass der Kunde der Verantwortliche (oder ein Auftragsverarbeiter, der personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet) ist und Cloudflare ein Auftragsverarbeiter (oder gegebenenfalls ein Unterauftragsverarbeiter) ist.

2.4 Wenn der Kunde ein Auftragsverarbeiter ist, sichert der Kunde Cloudflare zu, dass die Anweisungen und Handlungen des Kunden in Bezug auf die personenbezogenen Daten einschließlich der Ernennung von Cloudflare als weiterer Auftragsverarbeiter und, soweit zutreffend, der Abschluss der EU-SCC (inklusive eventueller Anpassungen gemäß Klauseln 6.2(b) und (c) unten) durch den jeweiligen Verantwortlichen genehmigt wurde (und für die Dauer dieses Nachtrags weiterhin genehmigt sein wird).

3. **Pflichten von Cloudflare**

3.1 Hinsichtlich aller personenbezogenen Daten, die Cloudflare in seiner Rolle als Auftragsverarbeiter oder Unterauftragsverarbeiter verarbeitet, wird Cloudflare :

(a) personenbezogene Daten nur für den beschränkten und spezifischen geschäftlichen Zweck verarbeiten, um den Dienst bereitzustellen, und nur in Einklang mit: (i) den schriftlichen Weisungen des Kunden, wie in dem Hauptvertrag und in diesem Nachtrag festgelegt, es sei denn, geltende Gesetze der EU oder eines EU-Mitgliedsstaates, denen Cloudflare unterliegt, verpflichten Cloudflare zu einer anderen Verarbeitung, und (ii) den Bestimmungen der Anwendbaren Datenschutzgesetze. Falls Cloudflare nach den Anwendbaren Datenschutzgesetzen zu einer Verarbeitung personenbezogener Daten verpflichtet ist, wird Cloudflare den Kunden vor einer solchen Verarbeitung über diese gesetzliche Verpflichtung informieren, es sei denn, das betreffende Gesetz verbietet eine solche Information aus wichtigen Gründen des öffentlichen Interesses;

(b) die personenbezogenen Daten nicht für Marketing- oder Werbezwecke nutzen wird;

(c) angemessene technische und organisatorische Maßnahmen umsetzen wird, um ein Sicherheitsniveau zu gewährleisten, das den durch die Verarbeitung personenbezogener Daten entstehenden Risiken angemessen ist, insbesondere einen Schutz gegen unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust, Veränderung, unbefugte Offenlegung von oder unbefugten Zugriff auf personenbezogene Daten. Diese Maßnahmen umfassen insbesondere die in Anhang 2 dargelegten Sicherheitsmaßnahmen („**Sicherheitsmaßnahmen**“). Der Kunde erkennt an, dass die Sicherheitsmaßnahmen technischem Fortschritt und technischer Entwicklung unterliegen und dass Cloudflare die Sicherheitsmaßnahmen von Zeit zu Zeit aktualisieren oder verändern kann, vorausgesetzt, dass solche Aktualisierungen und Veränderungen die Gesamtsicherheit des Dienstes nicht verringern oder senken;

(d) sicherstellen wird, dass nur autorisiertes Personal Zugriff auf solche personenbezogenen Daten hat und dass alle zum Zugriff auf personenbezogene Daten autorisierten Personen vertraglichen oder gesetzlichen Vertraulichkeitsverpflichtungen unterliegen;

(e) den Kunden unverzüglich nach Bekanntwerden einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise zum Zweck der Bereitstellung des Dienstes an den Kunden durch Cloudflare, einen Unterauftragsverarbeiter oder einen anderen bekannten oder unbekannten Dritten verarbeitet werden (eine „**Verletzung des Schutzes personenbezogener Daten**“), informieren und dem Kunden angemessene Kooperation und Unterstützung in Bezug auf diese Verletzung des Schutzes personenbezogener Daten bereitstellen, einschließlich angemessener Informationen im Besitz von Cloudflare, die sich auf diese Verletzung des Schutzes personenbezogener Daten beziehen, soweit sie die personenbezogenen Daten betreffen;

(f) ohne die vorherige schriftliche Zustimmung des Kunden keine öffentlichen Verlautbarungen über eine Verletzung des Schutzes personenbezogener Daten (eine „**Verletzungsmitteilung**“) veröffentlichen, es sei denn, dies ist, durch geltende Gesetze vorgeschrieben;

(g) soweit Cloudflare verifizieren kann, dass eine betroffene Person mit dem Kunden in Verbindung steht, dem Kunden unverzüglich melden, wenn Cloudflare den Antrag einer betroffenen Person auf Wahrnehmung von Datenschutzrechten (einschließlich der Rechte auf Auskunft, Berichtigung oder Löschung) in Bezug auf die personenbezogenen Daten dieser betroffenen Person erhält (einen „**Antrag einer betroffenen Person**"). Cloudflare darf ohne die vorherige schriftliche Zustimmung des Kunden nicht auf einen Antrag einer betroffenen Person antworten, abgesehen von einer Bestätigung, dass ein solcher Antrag sich auf den Kunden bezieht, wozu der Kunde hiermit zustimmt;

(h) soweit Cloudflare hierzu in der Lage ist und in Übereinstimmung mit geltendem Recht, dem Kunden bei der Beantwortung eines Antrags einer betroffenen Person auf Wahrnehmung von Datenschutzrechten gemäß den Anwendbaren Datenschutzgesetzen (einschließlich der Rechte auf Auskunft, Berichtigung oder Löschung) in Bezug auf die personenbezogenen Daten dieser betroffenen Person angemessene Unterstützung bereitstellen, falls der Kunde ohne die Unterstützung von Cloudflare nicht dazu in der Lage ist, einen Antrag einer betroffenen Person zu bearbeiten. Der Kunde ist dafür verantwortlich zu verifizieren, dass es sich bei dem Antragsteller um die betroffene Person handelt, auf deren personenbezogene Daten sich der gestellte Antrag bezieht. Cloudflare trägt keine Verantwortung für Informationen, die dem Kunden gemäß diesem Unterabschnitt in gutem Glauben zur Verfügung gestellt wurden. Der Kunde trägt alle Kosten, die Cloudflare in Verbindung mit der Bereitstellung einer solchen Unterstützung entstehen;

(i) soweit zur Einhaltung geltender Gesetze nicht anders erforderlich, nach Kündigung oder Ablauf des Hauptvertrags oder nach Beendigung des Dienstes alle personenbezogenen Daten (einschließlich aller Kopien davon), die gemäß dieses Nachtrags verarbeitet werden, nach Wahl des Kunden vernichten oder zurückgeben;

(j) unter Berücksichtigung der Art der Verarbeitung und der Cloudflare zur Verfügung stehenden Informationen, dem Kunden die Unterstützung gewähren, die der Kunde in Bezug auf Cloudflares Pflichten gemäß Anwendbaren Datenschutzgesetzen in Bezug auf:

(i) Datenschutz-Folgenabschätzungen und vorherige Konsultationen (wie in den Anwendbaren Datenschutzgesetzen definiert);

(ii) Benachrichtigungen der Aufsichtsbehörde gemäß den Anwendbaren Datenschutzgesetzen und/oder Mitteilungen an betroffene Personen durch den Kunden in Folge einer Verletzung des Schutzes personenbezogener Daten; und

(iii) die Einhaltung der Verpflichtungen des Kunden gemäß Anwendbarer Datenschutzgesetze in Bezug auf die Sicherheit der Verarbeitung;

vernünftigerweise verlangt, vorausgesetzt der Kunde trägt alle Kosten, die Cloudflare in Verbindung mit dieser Unterstützung entstehen; und

(k) den Kunden zu benachrichtigen, wenn nach Ansicht von Cloudflare durch den Kunden gemäß Klausel 3.1(a) erteilte Anweisungen gegen Anwendbare Datenschutzgesetze verstoßen oder Cloudflare aus einem anderen Grund feststellt seine Pflichten gemäß den Anwendbaren Datenschutzgesetzen nicht länger erfüllen zu können.

3.2 Soweit Cloudflare personenbezogene Daten im Anwendungsbereich des CCPA im Auftrag des Kunden verarbeitet, übernimmt Cloudflare die folgenden zusätzlichen Verpflichtungen gegenüber dem Kunden: Cloudflare wird die personenbezogenen Daten nicht für andere als die in dem Hauptvertrag und diesem Nachtrag dargelegten Zwecke und wie durch den CCPA, einschließlich einer sog. Verkaufsausnahme, erlaubt aufbewahren, nutzen oder offenlegen. Cloudflare wird personenbezogene Daten nicht verkaufen oder teilen, wie im CCPA definiert. Diese Klausel 3.2 lässt die Datenschutzverpflichtungen, die Cloudflare in dem Hauptvertrag oder diesem Nachtrag gegenüber dem Kunden übernimmt, unberührt.

3.3 Cloudflare bestätigt, dass es die in Klausel 2 und 3 sowie in den Anwendbaren Datenschutzgesetzen enthaltenen Verpflichtungen und Einschränkungen versteht und diese einhalten wird.

4. Unterauftragsverarbeitung

4.1 Cloudflare wird die personenbezogenen Daten nur für die spezifischen Zwecke der Bereitstellung der Dienste an Unterauftragsverarbeiter weitergeben.

4.2 Cloudflare wird sicherstellen, dass jeder Unterauftragsverarbeiter, der mit der Bereitstellung eines Teils des Dienstes in Verbindung mit diesem Nachtrag beauftragt wird, dies nur auf der Grundlage eines schriftlichen Vertrags tut, der dem Unterauftragsverarbeiter Bedingungen (d. h. Datenschutzpflichten) auferlegt, die einen gleichwertigen Schutz personenbezogener Daten gewährleisten im Vergleich mit den als Cloudflare in diesem Nachtrag auferlegten Bedingungen (die „**Relevanten Bedingungen**"). Cloudflare wird dafür Sorge tragen, dass der Unterauftragsverarbeiter die Relevanten Bedingungen erfüllt und haftet gegenüber dem Kunden für jeden Verstoß des Unterauftragsverarbeiters gegen die Relevanten Bedingungen.

4.3 Der Kunde erteilt eine allgemeine schriftliche Genehmigung: (a) an Cloudflare zur Einbeziehung anderer Unternehmen der Cloudflare-Unternehmensgruppe als Unterauftragsverarbeiter und (b) an Cloudflare und andere Unternehmen der Cloudflare-Unternehmensgruppe zur Einbeziehung dritter Rechenzentrumsbetreiber und Anbietern von Geschäfts-, Technik- und Kunden-Support als Unterauftragsverarbeiter zur Unterstützung der Bereitstellung des Dienstes .

4.4 Cloudflare führt unter https://www.cloudflare.com/gdpr/subprocessors/ eine Liste der Unterauftragsverarbeiter und fügt die Namen neuer und ersatzweise hinzukommender Unterauftragsverarbeiter mindestens dreißig (30) Tage vor dem Datum, an dem diese Unterauftragsverarbeiter mit der Verarbeitung personenbezogener Daten beginnen, zur Liste hinzu. Falls der Kunde einem neuen oder ersatzweise hinzukommenden Unterauftragsverarbeiter aus berechtigten datenschutzrechtlichen Gründen widerspricht, teilt er Cloudflare diesen Widerspruch innerhalb von zehn (10) Tagen nach der Benachrichtigung schriftlich mit und die Parteien werden versuchen, die Angelegenheit einvernehmlich zu lösen. Falls Cloudflare in der Lage ist, dem Kunden den Dienst in Einklang mit dem Hauptvertrag ohne den Einsatz des Unterauftragsverarbeiters bereitzustellen und sich nach eigenem Ermessen hierfür entscheidet, hat der Kunde keine weiteren Rechte gemäß dieser Klausel 4.4 in Bezug auf den vorgeschlagenen Einsatz des Unterauftragsverarbeiters. Falls Cloudflare nach eigenem Ermessen den Einsatz des Unterauftragsverarbeiters benötigt und nicht in der Lage ist, dem Widerspruch des Kunden bezüglich des vorgeschlagenen Einsatzes des neuen oder als Ersatz hinzugefügten Unterauftragsverarbeiters nachzukommen, kann der Kunde das entsprechende Bestellformular mit Gültigkeit zu dem Datum kündigen, an dem Cloudflare mit dem Einsatz des neuen oder ersatzweise hinzukommenden Unterauftragsverarbeiters beginnt, allerdings ausschließlich in Bezug auf den oder die Dienst(e) bei denen der vorgeschlagene neue Unterauftragsverarbeiter für die Verarbeitung personenbezogener Daten eingesetzt wird. Falls der Kunde keinen fristgerechten Widerspruch gemäß dieser Klausel 4.4 gegen einen neuen oder ersatzweise hinzukommenden Unterauftragsverarbeiter erhebt, gilt der Unterauftragsverarbeiter als vom Kunden akzeptiert und dessen Widerspruchsrecht als erloschen.

5. Audit und Aufzeichnungen

5.1 Cloudflare stellt dem Kunden gemäß Anwendbarer Datenschutzgesetze die Informationen zur Verfügung, die sich im Besitz oder unter der Kontrolle von Cloudflare befinden und die der Kunde zum Nachweis der Einhaltung der Pflichten von Unterauftragsverarbeitern nach den Anwendbaren Datenschutzgesetzen in Bezug auf die Verarbeitung personenbezogener Daten durch Cloudflare vernünftigerweise anfordern kann.

5.2 Cloudflare kann das Audit-Recht des Kunden gemäß den Anwendbaren Datenschutzgesetzen in Bezug auf personenbezogene Daten durch Bereitstellung des Folgenden erfüllen:

(a) einen Audit-Bericht, der nicht älter als dreizehn (13) Monate ist, von einem unabhängigen externen Prüfer erstellt wurde und nachweist, dass die technischen und organisatorischen Maßnahmen von Cloudflare ausreichend sind und einem akzeptierten Branchen-Audit-Standard entsprechen;

(b) zusätzliche Informationen, die sich im Besitz oder unter der Kontrolle von Cloudflare befinden, an eine Datenschutz-Aufsichtsbehörde, wenn diese zusätzliche Informationen in Bezug auf die Verarbeitung personenbezogener Daten durch Cloudflare im Rahmen dieses Nachtrags anfordert oder benötigt; und

(c) soweit die personenbezogenen Daten des Kunden den EU-SCC unterliegen und die gemäß dieser Klausel 5.2 zur Verfügung gestellten Informationen nach vernünftigem Ermessen des Kunden nicht ausreichend sind, um die Einhaltung der Pflichten von Cloudflare gemäß diesem Nachtrag oder den Anwendbaren Datenschutzgesetzen zu belegen, ermöglicht es Cloudflare dem Kunden, während der Laufzeit (wie in dem Hauptvertrag definiert) ein Vor-Ort-Audit pro Jahr zu verlangen, um die Einhaltung der Pflichten nach diesem Nachtrag durch Cloudflare gemäß Klausel 5.3 zu überprüfen.

5.3 Die folgenden zusätzlichen Bedingungen gelten für vom Kunden angeforderte Audits:

(a) Der Kunde muss alle Anfragen zur Prüfung der Audit-Berichte von Cloudflare an customer-compliance@cloudflare.com senden.

(b) Nach Eingang bei Cloudflare eines Audit-Verlangens gemäß Klausel 5.2(c) werden Cloudflare und der Kunde im Voraus das angemessene Startdatum, den Umfang, die Dauer und die Sicherheits- und Vertraulichkeitskontrollen für ein Audit gemäß Klausel 5.2(c) besprechen und vereinbaren. Soweit möglich, werden die Nachweise für ein solches Audit auf die Nachweise beschränkt, die im Rahmen des letzten Audits durch Dritte von Cloudflare eingeholt wurden.

(c) Cloudflare kann für ein Audit gemäß Klausel 5.2(c) eine Vergütung verlangen (basierend auf den angemessenen Kosten für Cloudflare). Vor einem solchen Audit wird Cloudflare dem Kunden weitere Einzelheiten zur anfallenden Vergütung und zur Grundlage ihrer Berechnung mitteilen. Der Kunde haftet für jegliche Vergütungen der von dem Kunden mit der Durchführung des Audits beauftragten Prüfer.

(d) Cloudflare kann einem vom Kunden mit der Durchführung eines Audits gemäß Klausel 5.2(c) beauftragten Prüfer schriftlich widersprechen, wenn der Prüfer nach Cloudflares vernünftiger Einschätzung nicht ausreichend qualifiziert oder unabhängig ist, ein Wettbewerber von Cloudflare oder anderweitig offensichtlich ungeeignet ist (d. h. ein Prüfer, dessen Beauftragung schädliche Auswirkungen auf das Geschäft von Cloudflare haben könnte, vergleichbar mit den vorgenannten Aspekten). Ein solcher Einwand durch Cloudflare verpflichtet den Kunden, einen anderen Prüfer zu beauftragen oder das Audit selbst durchzuführen. Finden die EU-SCC Anwendung (einschließlich eventueller Änderungen aufgrund der nachstehenden Klauseln 6.2(a) und (b)), so gilt, dass nichts in dieser Klausel 5.3 die EU-SCC ändert oder modifiziert oder die Rechte einer Aufsichtsbehörde oder betroffenen Person gemäß den EU-SCC beeinträchtigt.

6. Datenübermittlungen aus dem EWR, der Schweiz und dem Vereinigten Königreich

6.1 In Zusammenhang mit dem Dienst gehen die Parteien davon aus, dass Cloudflare (und seine Unterauftragsverarbeiter) bestimmte durch Europäische Datenschutzgesetze geschützte personenbezogene Daten, für die der Kunde oder ein Unternehmen der Unternehmensgruppe des Kunden Verantwortlicher (oder Auftragsverarbeiter im Auftrag eines Verantwortlichen) sein kann, außerhalb des Europäischen Wirtschaftsraums („**EWR**“), der Schweiz und des Vereinigten Königreichs verarbeiten kann.

6.2 Die Parteien vereinbaren, dass die Übermittlung durch Europäische Datenschutzgesetze geschützter personenbezogener Daten von dem Kunden oder einem Unternehmen der Unternehmensgruppe des

Kunden an Cloudflare, den entsprechenden EU-SCC wie folgt unterliegen muss, wenn es sich um eine Beschränkte Übermittlung handelt:

(a) **EU-Übermittlungen:** Für durch die EU-DSGVO geschützte personenbezogene Daten finden die EU-SCC wie folgt Anwendung:

(i) Modul 2gilt, wenn der Kunde (oder das entsprechende Unternehmen der Unternehmensgruppe des Kunden) ein Verantwortlicher ist, und Modul 3gilt, wenn der Kunde (oder das entsprechende Unternehmen der Unternehmensgruppe des Kunden) als ein Auftragsverarbeiter tätig ist;

(ii) in Klausel 7 gilt die optionale Kopplungsklausel;

(iii) in Klausel 9 gilt Option 2 und für die vorherige Benachrichtigung über die Änderung von Unterauftragsverarbeitern gilt der in Klausel 4.3 dieses Nachtrags dargelegte Zeitraum;

(iv) in Klausel 11 finden die optionalen Formulierungen keine Anwendung;

(v) in Klausel 17 gilt Option 2 und wenn der Mitgliedsstaat des Datenexporteurs keine Rechte als Drittbegünstigte zulässt, gilt deutsches Recht;

(vi) in Klausel 18(b) werden Streitigkeiten vor den Gerichten des Landes beigelegt, dessen Recht für den Hauptvertrag zwischen den Parteien gilt, oder, falls dieses Land kein EU-Mitgliedsstaat ist, vor den Gerichten in München, Deutschland. In jedem Fall gilt für die Klauseln 17 und 18 (b) einheitlich, dass die Rechts- und Gerichtswahl auf das Land des anwendbaren Rechts fällt;

(vii) Anhang I der EU-SCC gilt als mit den in Anhang 1 zu diesem Nachtrag aufgeführten Informationen ausgefüllt; und

(vii) Anhang II der EU-SCC gilt als mit den in Anhang 2 zu diesem Nachtrag aufgeführten Informationen ausgefüllt.

(b) **UK-Übermittlungen:** Für durch die UK-DSGVO geschützte personenbezogene Daten finden die EU-SCC gemäß Klausel 6.2(a) dieses Nachtrags Anwendung mit den folgenden Einschränkungen:

(i) die EU-SCC gelten wie durch das UK Addendum geändert, dass zwischen dem übermittelnden Kunden (oder dem entsprechenden Unternehmen der Unternehmensgruppe des Kunden) und Cloudflare als abgeschlossen gilt;

(ii) Widersprüche zwischen den Bedingungen der EU-SCC und dem UK Addendum werden nach Abschnitt 10 und Abschnitt 11 des UK Addendums gelöst;

(iii) die Tabellen 1 bis 3 in Teil 1 des UK Addendums gelten als mit den in den Anhängen dieses Nachtrags enthaltenen Informationen ausgefüllt; und

(iv) Tabelle 4 in Teil 1 des UK Addendums gilt als mit „keine der Parteien“ ausgefüllt.

(c) **Schweizer Übertragungen:** Für durch das Schweizer Datenschutzgesetz geschützte personenbezogene Daten finden die EU-SCC gemäß Klausel 6.2(a) dieses Nachtrags Anwendung mit den folgenden Einschränkungen:

(i) die zuständige Aufsichtsbehörde für solche personenbezogenen Daten ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte der Schweiz;

(ii) in Klausel 17 ist das anwendbare Recht das Schweizer Recht;

(iii) Bezugnahmen auf „Mitgliedsstaat(en)“ in den EU-SCC sind als Bezugnahme auf die Schweiz auszulegen und betroffene Personen, die sich in der Schweiz befinden, sind berechtigt, ihre Rechte im Rahmen der EU-SCC in der Schweiz auszuüben und durchzusetzen; und

(iv) Bezugnahmen auf „Datenschutz-Grundverordnung“, „Verordnung 2016/679“ oder „DSGVO“ in den EU-SCC sind als Bezugnahmen auf das Schweizer Datenschutzgesetz (in seiner aktuellen Fassung) auszulegen.

(d) Die folgenden Bestimmungen sind auf die EU-SCC anwendbar (einschließlich eventueller Änderungen aufgrund der vorstehenden Klauseln 6.2(a) und (b)):

(i) Der Kunde kann sein Audit-Recht aus den EU-SCC vorbehaltlich der Bestimmungen aus Klausel 5 dieses Nachtrags ausüben; und

(ii) Cloudflare kann Unterauftragsverarbeiter vorbehaltlich der Bestimmungen aus Klausel 4 und Klausel 6.3 dieses Nachtrags ernennen und der Kunde kann sein Recht auf Widerspruch gegen Unterauftragsverarbeiter gemäß den EU-SCC in der durch Klausel 4.3 dieses Nachtrags festgelegten Weise ausüben.

(e) Falls eine der Bestimmungen dieses Nachtrags, direkt oder indirekt in Widerspruch zu den EU-SCC (und dem UK Addendum, soweit anwendbar) steht, gehen Letztere vor.

6.3 Im Rahmen Beschränkter Übermittlungen an Cloudflare gemäß Klausel 6.2 darf Cloudflare nicht an weiteren Beschränkten Übermittlungen personenbezogener Daten (ob als „Exporteur“ oder „Importeur“ solcher personenbezogener Daten) teilnehmen (und keinem Unterauftragsverarbeiter eine Teilnahme gestatten), es sei denn, solche weiteren Beschränkten Übermittlungen erfolgen unter vollständiger Einhaltung der Europäischen Datenschutzgesetze und gemäß den zwischen dem Exporteur und Importeur der personenbezogenen Daten abgeschlossenen EU-SCC oder gemäß einem Alternativen Übermittlungsmechanismus (wie in Klausel 6.5 definiert) des Importeurs.

6.4 Falls der Kunde eine Bewertung der Angemessenheit der EU-SCC für Übermittlungen in bestimmte Länder oder Regionen durchführen möchte, wird Cloudflare, soweit möglich, dem Kunden für die Zwecke einer solchen Bewertung angemessene Unterstützung bereitstellen, vorausgesetzt, dass der Kunde alle Kosten trägt, die Cloudflare im Zusammenhang mit der Bereitstellung einer solchen Unterstützung entstehen.

6.5 Soweit Cloudflare einen alternativen Datenübermittlungsmechanismus (einschließlich einer gemäß den Anwendbaren Europäischen Datenschutzgesetzen eingeführten neuen Fassung oder eines Nachfolgers des *Privacy Shield*) für die Übermittlung personenbezogener Daten einführt, der nicht in diesem Nachtrag beschrieben ist („**Alternativer Übermittlungsmechanismus**“), gilt der Alternative Übermittlungsmechanismus anstelle des in diesem Nachtrag beschriebenen anwendbaren Übermittlungsmechanismus (jedoch nur soweit ein solcher Alternativer Übermittlungsmechanismus die Europäischen Datenschutzgesetze erfüllt und auf die Gebiete Anwendung findet, in die personenbezogene Daten übermittelt werden) und der Kunde stimmt zu, solche anderen und weiteren Dokumente zu unterzeichnen und solche anderen und weiteren Maßnahmen umzusetzen, wie vernünftigerweise erforderlich, um einem solchen Alternativen Übermittlungsmechanismus Rechtskraft zu verleihen.

7. Datenzugriffsanfragen von Drittparteien

7.1 Erlangt Cloudflare Kenntnis von einem rechtlichen Verfahren eines Dritten, in dem personenbezogene Daten angefordert werden, die Cloudflare als Auftragsverarbeiter oder Unterauftragsverarbeiter (wie jeweils zutreffend) im Auftrag des Kunden verarbeitet, wird Cloudflare:

(a) den Kunden unverzüglich über die Anfrage informieren, es sei denn, eine solche Information ist gesetzlich untersagt;

(b) den Dritten darüber informieren, dass Cloudflare Auftragsverarbeiter oder Unterauftragsverarbeiter (wie jeweils zutreffend) der personenbezogenen Daten ist und nicht befugt ist die personenbezogenen Daten ohne die Zustimmung des Kunden offenzulegen;

(c) dem Dritten nur die erforderlichen Kontaktdaten des Kunden mitteilen, damit der Dritte den Kunden kontaktieren kann, und wird den Dritten anweisen seine Anfrage an den Kunden zu richten; und

(d) soweit Cloudflare im Rahmen des rechtlichen Verfahrens eines Dritten Zugriff auf personenbezogene Daten gewährt oder diese offenlegt, entweder mit Zustimmung des Kunden oder aufgrund einer zwingenden rechtlichen Verpflichtung, wird Cloudflare die personenbezogenen Daten auf das aufgrund der rechtlichen Verpflichtung notwendige Maß beschränkt und in Einklang mit dem entsprechenden rechtlichen Verfahren offenlegen.

7.2 Von Cloudflare kann in seiner Rolle als Auftragsverarbeiter oder Unterauftragsverarbeiter, soweit jeweils zutreffend, im Zusammenhang mit einem rechtlichen Verfahren eines Dritten durch eine Regierungsbehörde (einschließlich Justizbehörden) der Zugriff auf oder die Offenlegung von personenbezogenen Daten angefordert werden. Erlangt Cloudflare von einem rechtlichen Verfahren eines Dritten Kenntnis, in dessen Zusammenhang von Cloudflare durch eine Regierungsbehörde (einschließlich Justizbehörden) der Zugriff auf oder die Offenlegung von personenbezogenen Daten angefordert wird, die Cloudflare im Auftrag des Kunden in seiner Rolle als Auftragsverarbeiter oder Unterauftragsverarbeiter (soweit jeweils zutreffend) verarbeitet, wird Cloudflare, soweit Cloudflare die Anforderung mit vernünftigem Aufwand geprüft hat und zu dem Schluss kommt, dass die Anforderung der personenbezogenen Daten im Zusammenhang mit diesem rechtlichen Verfahren einen Verstoß gegen das Gesetz verursacht:

(a) alle in Klausel 7.1 oben genannten Maßnahmen umsetzen;

(b) Rechtsmittel bis zur Stufe eines Berufungsgerichts einlegen, bevor personenbezogene Daten offengelegt werden; und

(c) keine personenbezogenen Daten offenlegen, bis (und dann nur in dem Umfang, in dem) es hierzu unter den geltenden Verfahrensregeln verpflichtet ist.

7.3 Die Klauseln 7.1 und 7.2 gelten nicht für den Fall, dass Cloudflare in gutem Glauben annimmt, dass die Anfrage einer Regierungsbehörde aufgrund eines Notfalls erforderlich ist, der Lebensgefahr oder die Gefahr schwerwiegender Verletzungen für eine Einzelperson mit sich bringt. In einem solchen Fall wird Cloudflare den Kunden so bald wie möglich nach der Offenlegung über die Datenweitergabe informieren und dem Kunden sämtliche Einzelheiten derselben zur Verfügung stellen, es sei denn, eine solche Informationsweitergabe ist gesetzlich untersagt.

7.4 Cloudflare wird dem Kunden regelmäßige Aktualisierungen über rechtliche Verfahren von Dritten, in deren Rahmen personenbezogene Daten angefordert wurden, bereitstellen, in Form des halbjährlichen Cloudflare-Transparenzberichts der unter https://www.cloudflare.com/transparency/ verfügbar ist.

7.5 Zu dem Datum, an dem der Kunde diesen Nachtrag mit Cloudflare abgeschlossen hat, gibt Cloudflare die folgenden Zusicherungen ab. Cloudflare wird diese Zusicherungen bei Bedarf unter https://www.cloudflare.com/transparency/ aktualisieren:

(a) Wir haben niemals unsere Kryptographie- oder Authentifizierungsschlüssel oder die unserer Kunden weitergegeben.

(b) Wir haben niemals Software oder Geräte von Strafverfolgungsbehörden auf unserem Netzwerk installiert.

(c) Wir haben niemals einen Feed der Inhalte unserer Kunden, die unser Netzwerk durchlaufen, einer Strafverfolgungsbehörde zugänglich gemacht.

(d) Wir haben niemals unsere Verschlüsselung auf Ersuchen von Strafverfolgungsbehörden oder anderen Dritten abgeschwächt, beeinträchtigt oder unterlaufen.

8. Allgemein

8.1 Dieser Nachtrag berührt nicht die Rechte und Pflichten der Parteien im Rahmen des Hauptvertrags, welche weiterhin vollständig in Kraft bleibt. Im Falle von Widersprüchen zwischen den Bedingungen dieses Nachtragsund den Bedingungen des Hauptvertrags haben die Bedingungen dieses Nachtrags Vorrang, soweit es um die Verarbeitung personenbezogener Daten geht.

8.2 Die Haftung von Cloudflare unter oder in Zusammenhang mit diesem Nachtrag, einschließlich der EU-SCC, unterliegt den Haftungsausschlüssen und -beschränkungen in dem Hauptvertrag. In keinem Fall beschränkt Cloudflare seine Haftung gegenüber betroffenen Personen oder zuständigen Datenschutzbehörden oder schließt diese aus.

8.3 Mit Ausnahme der Fälle und soweit dies in den EU-SCC ausdrücklich vorgesehen oder aufgrund der Anwendbaren Datenschutzgesetze vorgeschrieben ist, gewährt dieser Nachtrag Dritten keine Rechte als Begünstigte; Er gilt ausschließlich zu Gunsten der Parteien dieses Nachtrags sowie ihrer jeweiligen gesetzlichen Rechtsnachfolger und Abtretungsempfänger und nicht zu Gunsten einer anderen Person und keine ihrer Bestimmungen kann von einer anderen Person durchgesetzt werden.

8.4 Dieser Nachtrag und alle damit zusammenhängenden Handlungen unterliegen den in dem Hauptvertrag angegebenen Gesetzen und sind nach diesen auszulegen, ohne Anwendung des Kollisionsrechts. Die Parteien stimmen der persönlichen Zuständigkeit und dem Gerichtsstand der in dem Hauptvertrag festgelegten Gerichte zu.

8.5 Sollte eine Bestimmung dieses Nachtrags aus irgendeinem Grund für ungültig oder undurchsetzbar erklärt werden, bleiben die anderen Bestimmungen des Nachtrags durchsetzbar. Ohne die Allgemeingültigkeit des Vorstehenden einzuschränken, erklärt sich der Kunde damit einverstanden, dass Klausel 8.2 (Haftungsbeschränkung) ungeachtet der Nichtdurchsetzbarkeit einer Bestimmung in diesem Nachtrag in Kraft bleibt.

8.6 Dieser Nachtrag stellt die endgültige, vollständige und ausschließliche Vereinbarung der Parteien in Bezug auf den Gegenstand dieses Nachtrags dar und ersetzt alle früheren Gespräche und Vereinbarungen zwischen den Parteien in Bezug auf diesen Gegenstand.

Anhang 1

Beschreibung der Datenverarbeitung

Dieser Anhang 1 ist Teil des Nachtrags und beschreibt die Verarbeitung, die Cloudflare im Auftrag des Kunden durchführt.

A. LISTE DER PARTEIEN

Datenexporteur(e): *Der Kunde füllt die rechte Spalte aus.*

1.	Name: *Der Kunde und alle Verbundenen Unternehmen des Kunden, die in dem Hauptvertrag beschrieben sind.*	Wie in dem Hauptvertrag aufgeführt.
	Anschrift: *Adressen des Kunden und aller Verbundenen Unternehmen des Kunden, die in dem Hauptvertrag beschrieben sind (oder Cloudflare sonst durch den Kunden mitgeteilt wurden).*	Wie in dem Hauptvertrag aufgeführt.
	Name, Funktion und Kontaktdaten der Kontaktperson:	Wie in dem Hauptvertrag aufgeführt.
	Tätigkeiten, die für die gemäß diesem Nachtrag und der EU-SCC übermittelten Daten von Belang sind:	Nutzung des Dienstes gemäß dem Hauptvertrag.
	Unterschrift und Datum:	Dieser Anhang 1 gilt bei Unterzeichnung des Nachtrags als unterzeichnet.
	Rolle (Verantwortlicher/Auftragsverarbeiter):	Verantwortlicher (oder Auftragsverarbeiter im Auftrag eines dritten Verantwortlichen).

Datenimporteur(e):

1.	Name:	Cloudflare, Inc.
	Anschrift:	101 Townsend Street San Francisco, CA 94107 USA
	Name, Funktion und Kontaktdaten der Kontaktperson:	Emily Hancock Data Protection Officer legal@cloudflare.com

	Tätigkeiten, die für die gemäß diesem Nachtrag und der EU-SCC übermittelten Daten von Belang sind:	Notwendige Verarbeitung zur Bereitstellung des Dienstes für den Kunden gemäß dem Hauptvertrag.
	Unterschrift und Datum:	Dieser Anhang 1 gilt bei Unterzeichnung des Nachtrags als unterzeichnet.
	Rolle (Verantwortlicher/Auftragsverarbeiter):	Auftragsverarbeiter (oder Unterauftragsverarbeiter)

B. BESCHREIBUNG DER DATENVERARBEITUNG UND -ÜBERMITTLUNG

Kategorien betroffener Personen, deren personenbezogene Daten übermittelt werden:	Natürliche Personen, die (i) auf die Domains, Netzwerke, Websites, Anwendungs-Programmierschnittstellen („APIs“) und Anwendungen des Kunden zugreifen oder diese nutzen, oder (ii) Mitarbeiter, Vertreter oder Auftragnehmer des Kunden, die auf die Dienste zugreifen oder diese nutzen, z. B. Endbenutzer des Zero Trust-Diensts von Cloudflare (gemeinsam: „Endbenutzer“). Natürliche Personen mit Zugangsdaten für ein Cloudflare-Konto und/oder Personen, die einen der Dienste für einen Kunden verwalten („Administratoren“).
Kategorien der übermittelten personenbezogenen Daten:	In Bezug auf Endbenutzer: ● Jedwede personenbezogenen Daten, die in den Protokollen des Kunden verarbeitet werden, wie beispielsweise IP-Adressen, und im Falle von Cloudflare Zero Trust, die Namen und E-Mail-Adressen der Endbenutzer von Cloudflare Zero Trust. „Protokolle des Kunden“ bezeichnet sämtliche Protokolle der Interaktionen der Endbenutzer mit den Internet-Eigenschaften des Kunden und dem Dienst, der dem Kunden über das Dashboard des Dienstes oder sonstige Online-Schnittstellen während der Laufzeit durch Cloudflare zur Verfügung gestellt wurde. ● Alle in Kundeninhalten verarbeiteten personenbezogenen Daten, deren Umfang vom Kunden nach dessen alleinigem Ermessen festgelegt und kontrolliert wird. „Kundeninhalt“ bezeichnet alle Dateien, Software, Skripte, Multimedia-Bilder, Grafiken, Audio, Video, Text, Daten oder andere Objekte, die von Websites stammen oder durch sie übertragen werden, die sich im

	Besitz des Kunden befinden, von ihm kontrolliert oder betrieben werden oder von ihm über den Dienst hochgeladen werden, und die an das Cloudflare-Netzwerk oder innerhalb des Cloudflare-Netzwerks weitergeleitet, weitergegeben, verarbeitet und/oder dort zwischengespeichert werden oder anderweitig über den Dienst durch den Kunden übertragen oder weitergeleitet werden. In Bezug auf Benutzer mit Administratorenzugriff: ● Sämtliche personenbezogenen Daten, die in den Audit-Protokollen von Benutzern mit Administratorenzugriff verarbeitet werden, wie beispielsweise IP-Adressen und E-Mail-Adressen.
Übertragene sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z.B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnung über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen:	Der Kunde, seine Endbenutzer, Administratoren und/oder anderen Partner können auf die Online-Websites des Kunden Inhalte hochladen, welche möglicherweise besondere Datenkategorien umfassen, deren Umfang vom Kunden nach eigenem Ermessen festgelegt und kontrolliert wird. Diese besonderen Datenkategorien umfassen unter Umständen u. a. Informationen über die ethnische Herkunft, politische Ansichten, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit und die Verarbeitung von Daten über die Gesundheit oder das Sexualleben einer Einzelperson. Alle dieser besonderen Kategorien von Daten sind durch die Anwendung der in Anhang 2 beschriebenen Sicherheitsmaßnahmen zu schützen.
Häufigkeit der Übermittlung (z. B. ob die Daten einmalig oder kontinuierlich übermittelt werden):	Fortlaufend während der Laufzeit des Hauptvertrags.
Art der Verarbeitung:	Notwendige Verarbeitung zur Bereitstellung der Dienste für den Kunden gemäß den in dem Hauptvertrag und diesem Nachtrag dokumentierten Anweisungen.
Zweck(e) der Datenübermittlung und Weiterverarbeitung:	Notwendige Verarbeitung zur Bereitstellung der Dienste für den Kunden gemäß den in dem Hauptvertrag und diesem Nachtrag dokumentierten Anweisungen.

Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieses Dauer:	Bis zum früheren folgender Zeitpunkte: (i) Ablauf/Kündigung des Hauptvertrags oder (ii) Datum, an dem die Verarbeitung für die Parteien nicht mehr erforderlich ist, um ihre Verpflichtungen aus dem Hauptvertrag zu erfüllen (soweit anwendbar).
Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben:	Gegenstand, Art und Dauer der Verarbeitung sind in dem Hauptvertrag festgelegt.

C. ZUSTÄNDIGE AUFSICHTSBEHÖRDE

Angabe der zuständigen Aufsichtsbehörde(n) (z. B. gemäß Klausel 13 der EU-SCC)	Bezeichnet in Bezug auf die EU-SCC die zuständige Aufsichtsbehörde, die gemäß Klausel 13 der EU-SCC festgelegt wurde. Bezeichnet in Bezug auf UK Addendum das Information Commissioner‘s Office des Vereinigten Königreichs.

Anhang 2

Technische und organisatorische Sicherheitsmaßnahmen

Cloudflare hat ein Informationssicherheitsprogramm gemäß ISO/IEC-27000-Standards eingerichtet und erhält dieses aufrecht. Das Sicherheitsprogramm von Cloudflare umfasst:

Maßnahmen zur Verschlüsselung personenbezogener Daten

Cloudflare setzt eine Verschlüsselung ein, um persönliche Daten angemessen zu schützen, und zwar unter Verwendung von:

- Verschlüsselungsprotokollen nach dem neuesten Stand der Technik, die einen wirksamen Schutz gegen aktive und passive Angriffe mit Ressourcen bieten, von denen bekannt ist, dass sie öffentlichen Behörden zur Verfügung stehen;
- vertrauenswürdigen Zertifizierungsstellen und Infrastrukturen für öffentliche Schlüssel;
- effektiven Verschlüsselungsalgorithmen und Parametrisierung, wie z. B. Mindestlängen von 128-Bit für symmetrische Verschlüsselung und mindestens 2048-Bit-RSA oder 256-Bit-ECC für asymmetrische Algorithmen.

Maßnahmen zur Gewährleistung der kontinuierlichen Vertraulichkeit, Integrität, Verfügbarkeit und Widerstandsfähigkeit von Verarbeitungssystemen und Diensten

Cloudflare verbessert die Sicherheit der Verarbeitungssysteme und Dienste in Produktionsumgebungen durch:

- Einsatz eines Code-Review-Prozesses zur Erhöhung der Sicherheit des für die Bereitstellung der Dienste verwendeten Codes sowie Testcode und -systeme für Schwachstellen vor und während der Nutzung;
- Unterhaltung eines externen Bug-Bounty-Programms;
- Prüfungen zur Validierung der Integrität verschlüsselter Daten; und
- Einsatz präventiver und reaktiver Angriffserkennung.

Cloudflare stellt hochverfügbare Systeme in geografisch verteilten Rechenzentren bereit.

Cloudflare setzt Eingabekontrollmaßnahmen ein, um die Vertraulichkeit personenbezogener Daten zu schützen und zu wahren, einschließlich:

- einer Autorisierungsrichtlinie für die Eingabe, das Lesen, Verändern und Löschen von Daten;
- der Authentifizierung autorisierter Mitarbeiter unter Verwendung eindeutiger Authentifizierungsdaten (Passwörter) und von Hardware-Token;
- der automatischen Abmeldung von Benutzerkennungen nach einem festgelegten Inaktivitätszeitraum;
- des Schutzes der Dateneingabe sowie des Lesens, der Veränderung und der Löschung gespeicherter Daten; und
- der Vorschrift, dass Datenverarbeitungseinrichtungen (die Räume, die die Computerhardware und zugehörige Ausrüstung enthalten) verschlossen und gesichert bleiben.

Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit von und den Zugang zu personenbezogenen Daten im Falle eines physischen oder technischen Zwischenfalls zeitnah wiederherzustellen

Cloudflare setzt Maßnahmen ein, um sicherzustellen, dass personenbezogene Daten vor versehentlicher Zerstörung oder Verlust geschützt sind, unter anderem durch die Aufrechterhaltung von:

- Notfallwiederherstellungs- und Geschäftsweiterführungsplänen und -verfahren;
- geografisch verteilten Rechenzentren;
- redundanter Infrastruktur einschließlich Stromversorgung und Internetverbindung;

- Sicherheitskopien, die an alternativen Standorten gespeichert werden und zur Wiederherstellung bei Ausfall primärer Systeme verwendet werden können; und
- Vorfallsmanagement-Verfahren, die regelmäßig getestet werden.

Prozesse zur regelmäßigen Prüfung, Bewertung und Evaluierung der Wirksamkeit technischer und organisatorischer Maßnahmen, um die Sicherheit der Verarbeitung zu gewährleisten

Die technischen und organisatorischen Maßnahmen von Cloudflare werden als Teil des Sicherheits- und Datenschutz-Compliance-Programms von Cloudflare regelmäßig von externen Prüfern getestet und bewertet. Dies kann jährliche ISO/IEC-27001-Audits, AICPA SOC 2 Typ II, PCI DSS Level 1 und andere externe Audits umfassen. Maßnahmen werden weiterhin regelmäßig durch interne Audits sowie jährliche und gezielte Risikobewertungen geprüft.

Maßnahmen zur Nutzeridentifikation und -autorisierung

Cloudflare implementiert wirksame Maßnahmen für die Benutzerauthentifizierung und Berechtigungsverwaltung durch:

- Anwendung einer obligatorischen Zugriffskontroll- und Authentifizierungsrichtlinie;
- Anwendung eines Zero-Trust-Modells für Identifizierung und Autorisierung;
- Authentifizierung autorisierter Mitarbeiter mithilfe einzigartiger Authentifizierungsdaten und einer starken Multi-Faktor-Authentifizierung, einschließlich der Verwendung physischer Hardware-Token;
- Zuweisung und Verwaltung geeigneter Berechtigungen in Einklang mit Funktion, Genehmigungen und Ausnahmemanagement; und
- Anwendung des Grundsatzes des minimalen Zugangs („Least Privilege“).

Maßnahmen zum Schutz von Daten während ihrer Übermittlung

Cloudflare setzt wirksame Maßnahmen ein, um personenbezogene Daten bei ihrer Übermittlung davor zu schützen, von unbefugten Personen gelesen, kopiert, verändert oder gelöscht zu werden, unter anderem durch:

- Einsatz von Transport-Verschlüsselungsprotokollen nach dem neuesten Stand der Technik, die einen wirksamen Schutz gegen aktive und passive Angriffe mit Ressourcen bieten, von denen bekannt ist, dass sie öffentlichen Behörden zur Verfügung stehen;
- Einsatz vertrauenswürdiger Zertifizierungsstellen und Infrastrukturen für öffentliche Schlüssel;
- Umsetzung von Schutzmaßnahmen gegen aktive und passive Angriffe auf die Sende- und Empfangssysteme, die Transportverschlüsselung zur Verfügung stellen, z. B. geeignete Firewalls, gegenseitige TLS-Verschlüsselung, API-Authentifizierung und Verschlüsselung zum Schutz der Gateways und Pipelines, durch die sich Daten bewegen, sowie Prüfungen auf Software-Schwachstellen und mögliche Software-Hintertüren;
- Einsatz effektiver Verschlüsselungsalgorithmen und Parametrisierung, wie z. B. Mindestlängen von 128-Bit für symmetrische Verschlüsselung und mindestens 2048-Bit-RSA oder 256-Bit-ECC für asymmetrische Algorithmen;
- Verwendung korrekt implementierter und ordnungsgemäß gewarteter Software, abgedeckt im Rahmen eines Schwachstellenmanagement-Programms und durch Audits auf Konformität geprüft;
- Durchsetzung von Sicherheitsmaßnahmen zur zuverlässigen Erstellung, Verwaltung, Speicherung und zum Schutz von Kodierungsschlüsseln; und
- Auditprotokolle, Überwachung und Nachverfolgung von Datenübermittlungen.

Maßnahmen zum Schutz von Daten während ihrer Speicherung

Cloudflare setzt wirksame Maßnahmen zum Schutz persönlicher Daten während ihrer Speicherung und zur Kontrolle und Begrenzung des Zugangs zu Datenverarbeitungssystemen ein, außerdem durch:

- Einsatz von Verschlüsselungsprotokollen nach dem neuesten Stand der Technik, die einen wirksamen Schutz gegen aktive und passive Angriffe mit Ressourcen bieten, von denen bekannt ist, dass sie öffentlichen Behörden zur Verfügung stehen;
- Einsatz vertrauenswürdiger Zertifizierungsstellen und Infrastrukturen für öffentliche Schlüssel;
- Prüfung von Datenspeichersystemen auf Software-Schwachstellen und mögliche Hintertüren;
- Einsatz wirksamer Verschlüsselungsalgorithmen und Parametrisierung, z. B. die Vorschrift, alle Festplatten, auf denen persönliche Daten gespeichert sind, mit AES-XTS mit einer Schlüssellänge von 128-Bit oder länger zu verschlüsseln.
- Verwendung korrekt implementierter und ordnungsgemäß gewarteter Software, abgedeckt im Rahmen eines Schwachstellenmanagement-Programms und durch Audits auf Konformität geprüft;
- Durchsetzung von Sicherheitsmaßnahmen zur zuverlässigen Erstellung, Verwaltung, Speicherung und zum Schutz von Kodierungsschlüsseln;
- Identifizierung und Genehmigung von Systemen und Benutzern mit Zugang zu Datenverarbeitungssystemen;
- Automatische Abmeldung von Benutzern nach einem festgelegten Inaktivitätszeitraum; und
- Audit-Protokollierung, Überwachung und Nachverfolgung des Zugriffs auf Datenverarbeitungs- und Speichersysteme.

Cloudflare setzt Zugriffskontrollen für bestimmte Bereiche der Datenverarbeitungssysteme ein, um sicherzustellen, dass nur befugte Nutzer in dem Rahmen und Umfang Zugriff auf personenbezogene Daten erhalten, der durch ihre jeweilige Zugriffsberechtigung (Autorisierung) abgedeckt ist, und dass personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Dies wird durch verschiedene Maßnahmen gewährleistet, darunter:

- Mitarbeiterrichtlinien und -schulungen in Bezug auf die Zugriffsrechte der Mitarbeiter auf persönliche Daten;
- Anwendung eines Zero-Trust-Modells für die Identifizierung und Autorisierung von Benutzern;
- Authentifizierung autorisierter Mitarbeiter mithilfe einzigartiger Authentifizierungsdaten und einer starken Multi-Faktor-Authentifizierung, einschließlich der Verwendung physischer Hardware-Token;
- Überwachung der Handlungen von Personen, die befugt sind, persönliche Daten zu löschen, hinzuzufügen oder zu verändern;
- Freigabe von Daten nur an befugte Personen, einschließlich der Zuordnung differenzierter Zugriffsrechte und Rollen; und
- Kontrolle des Zugriffs auf Daten mit kontrollierter und dokumentierter Vernichtung von Daten.

Maßnahmen zur Gewährleistung der physischen Sicherheit von Standorten, an denen personenbezogene Daten verarbeitet werden

Cloudflare unterhält und implementiert wirksame Richtlinien und Maßnahmen für physische Zugangskontrollen, um zu verhindern, dass unbefugte Personen Zugang zu den Datenverarbeitungseinrichtungen (namentlich Datenbank- und Anwendungsserver und zugehörige Hardware) erhalten, auf denen personenbezogene Daten verarbeitet oder genutzt werden, unter anderem durch:

- Einrichtung sicherer Bereiche;
- Schutz und Beschränkung von Zugangswegen;
- Festlegung von Zugriffsberechtigungen für Mitarbeiter und Dritte, einschließlich der entsprechenden Dokumentation;
- jeder Zugang zu Rechenzentren, in denen persönliche Daten gespeichert werden, wird protokolliert, überwacht und nachverfolgt; und
- Rechenzentren, in denen persönliche Daten gespeichert werden, sind durch Sicherheitsmeldesysteme und andere geeignete Sicherheitsmaßnahmen gesichert.

Maßnahmen zur Sicherstellung der Protokollierung von Ereignissen

Cloudflare hat ein Protokoll- und Überwachungsprogramm für die Protokollierung, Überwachung und Nachverfolgung des Zugriffs auf personenbezogene Daten, unter anderem durch Systemadministratoren, und zur Sicherstellung, dass Daten in Einklang mit erhaltenen Anweisungen verarbeitet werden, eingeführt. Dies wird durch verschiedene Maßnahmen erreicht, darunter:

- Authentifizierung autorisierter Mitarbeiter mithilfe einzigartiger Authentifizierungsdaten und einer starken Multi-Faktor-Authentifizierung, einschließlich der Verwendung physischer Hardware-Token;
- Anwendung eines Zero-Trust-Modells für die Identifizierung und Autorisierung von Benutzern;
- Führung aktueller Listen mit den Identifikationsdaten der Systemadministratoren;
- Umsetzung von Maßnahmen zur Erkennung, Bewertung und Reaktion auf Hochrisiko-Anomalien;
- Führung sicherer, genauer und unveränderter Protokolle der Zugriffe auf die Verarbeitungsinfrastruktur für einen Zeitraum von zwölf Monaten; und
- Prüfung der Protokollkonfiguration, des Überwachungssystems, der Melde- und Vorfallsreaktionsverfahren mindestens einmal jährlich.

Maßnahmen zur Sicherstellung der Systemkonfiguration, einschließlich der Standardkonfiguration

Cloudflare unterhält Konfigurationsstandards für alle Systeme, die die Produktionsdatenverarbeitungsumgebung unterstützen, einschließlich Drittanbietersysteme. Konfigurationsstandards sollten den branchenüblichen bewährten Praktiken wie den Maßstäben des *Center for Internet Security (CIS) Level 1* entsprechen. Automatisierte Mechanismen müssen eingesetzt werden, um die Basiskonfigurationen auf Produktionssystemen durchzusetzen und um unbefugte Änderungen zu verhindern. Änderungen der Standards sind auf eine geringe Anzahl autorisierter Mitarbeiter von Cloudflare beschränkt und müssen die Änderungskontrollprozesse befolgen. Änderungen müssen nachvollziehbar sein und regelmäßig überprüft werden, um Abweichungen von Ausgangskonfigurationen festzustellen.

Cloudflare konfiguriert die Standards für das Informationssystem unter Anwendung des Grundsatzes der geringsten Privilegien („Least Privilege“). Standardmäßig werden Zugriffskonfigurationen auf „deny-all“ (alle ablehnen) gesetzt und Standardpasswörter müssen vor der Geräteinstallation im Cloudflare-Netzwerk oder unmittelbar nach der Software- oder Betriebssysteminstallation geändert werden, um die Richtlinien von Cloudflare zu erfüllen. Die Systeme sind so eingerichtet, dass die Systemzeituhren auf Grundlage der Internationalen Atomzeit oder der koordinierten Universalzeit (UTC) synchronisiert werden, und der Zugriff auf Zeitdaten ist auf autorisiertes Personal beschränkt.

Maßnahmen für Regelung und Verwaltung der internen IT und IT-Sicherheit

Cloudflare unterhält interne Richtlinien zur akzeptablen Nutzung von IT-Systemen und zur allgemeinen Informationssicherheit. Cloudflare verlangt von allen Mitarbeitern, dass sie mindestens einmal im Jahr an einer allgemeinen Schulung zum Thema Sicherheit und Datenschutz teilnehmen. Cloudflare beschränkt und schützt die Verarbeitung persönlicher Daten und hat Folgendes dokumentiert und umgesetzt:

- ein formales Informationssicherheits-Verwaltungssystem (ISMS), um die Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit der Daten und Informationssysteme von Cloudflare zu schützen und die Wirksamkeit der Sicherheitskontrollen über Daten und Informationssysteme zu gewährleisten, die den Betrieb unterstützen; und
- ein formales Datenschutz-Informationsverwaltungssystem (PIMS) zum Schutz der Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit der Richtlinien und Verfahren, die das globale verwaltete Netzwerk von Cloudflare unterstützen, sowohl als Auftragsverarbeiter als auch als Verantwortlicher für Kundendaten.

Cloudflare bewahrt Dokumentationen über technische und organisatorische Maßnahmen für den Fall von Audits und zur Beweissicherung auf. Cloudflare trifft angemessene Maßnahmen, um zu gewährleisten, dass von Cloudflare beschäftigte Personen und andere Personen am betroffenen Arbeitsplatz die in diesem Anhang 2 beschriebenen technischen und organisatorischen Maßnahmen kennen und einhalten.

Maßnahmen zur Zertifizierung/Prüfung von Prozessen und Produkten

Die Implementierung des ISMS von Cloudflare und der zugehörigen Sicherheitsrisikomanagementprozesse wurden extern nach dem Branchenstandard ISO/IEC 27001 zertifiziert. Die Umsetzung des umfassenden PIMS von Cloudflare wurde extern nach dem Branchenstandard ISO/IEC 27701 zertifiziert, sowohl für Cloudflare als Auftragsverarbeiter als auch als Verantwortlicher für Kundeninformationen.

Cloudflare hält seine Konformität mit PCI DSS Level 1 aufrecht, für die Cloudflare jährlich von einem externen qualifizierten Sicherheitsgutachter geprüft wird. Cloudflare hat weitere Zertifizierungen wie AICPA SOC 2 Typ II nach den AICPA-Trust-Service-Kriterien absolviert. Einzelheiten zu diesen und anderen Zertifizierungen, die Cloudflare von Zeit zu Zeit absolviert, werden auf der Website von Cloudflare zur Verfügung gestellt.

Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch die spezifischen technischen und organisatorischen Maßnahmen zu beschreiben, die der (Unter-)Auftragsverarbeiter zur Unterstützung des Verantwortlichen und (bei Datenübermittlungen von einem Auftragsverarbeiter an einen Unterauftragsverarbeiter) zur Unterstützung des Datenexporteurs ergreifen muss.

Maßnahme	**Beschreibung**
Selbstbedienungszugriff, um die Rechte betroffener Personen auf Zugriff, Löschung, Berichtigung usw. zu erfüllen.	Möglichkeit der Anmeldung, um persönliche Daten über das Cloudflare-Dashboard zu prüfen und zu bearbeiten.