NACHTRAG ZUR DATENVERARBEITUNG CLOUDFLARE

Cloudflare, Inc. („**Cloudflare**“) und die diesen Bedingungen zustimmende Vertragspartei („**Kunde“**), haben einen Enterprise Subscription Vertrag, einen Self-Serve Subscription Vertrag oder eine andere schriftliche oder elektronische Vereinbarung für die von Cloudflare bereitgestellten Dienste abgeschlossen (der „**Hauptvertrag“**). Dieser Nachtrag zur Datenverarbeitung**,** einschließlich dessen Anhänge (der **„NDV“)** ist Bestandteil des Hauptvertrages.

Dieser NDV tritt ab dem Datum in Kraft und ersetzt alle zuvor anwendbaren Bedingungen in Bezug auf seinen Gegenstand (einschließlich Änderungen, Vereinbarungen oder Ergänzungen der Datenverarbeitung in Bezug auf die Dienstleistungen), an dem der Kunde dieses NDV unterzeichnet oder die Parteien anderweitig diesem NDV zugestimmt haben („**NDV-Wirksamkeitsdatum“**).

Wenn Sie dieses DPA im Namen des Kunden akzeptieren, garantieren Sie, dass: (a) Sie die volle rechtliche Befugnis haben, den Kunden an dieses DPA zu binden; (b) Sie dieses DPA gelesen und verstanden haben; und (c) Sie im Namen des Kunden diesem DPA zustimmen. Wenn Sie nicht die rechtliche Befugnis haben, den Kunden an dieses DPA zu binden, akzeptieren Sie dieses DPA bitte nicht.

DATENVERARBEITUNGSBEDINGUNGEN

Dieser NDV gilt, wenn Cloudflare Personenbezogene Daten als Auftragsverarbeiter (oder gegebenenfalls Unterauftragsverarbeiter) im Namen des Kunden verarbeitet und diese Personenbezogenen Daten den geltenden Datenschutzgesetzen (wie unten definiert) unterliegen.

Die Parteien haben vereinbart, diesen NDV zu schließen, um sicherzustellen, dass geeignete Schutzmaßnahmen getroffen werden, um diese Personenbezogenen Daten in Übereinstimmung mit den geltenden Datenschutzgesetzen zu schützen. Daher erklärt sich Cloudflare damit einverstanden, die folgenden Bestimmungen in Bezug auf alle Personenbezogenen Daten, die Cloudflare als Auftragsverarbeiter (oder gegebenenfalls Unterauftragsverarbeiter) für den Kunden verarbeitet, einzuhalten.

1. Definitionen

1.1 In diesem NDV werden folgende Definitionen verwendet:

a) „**Angemessenes Land**“ bezeichnet ein Land oder ein Gebiet, das gemäß den Europäischen Datenschutzgesetzen anerkannt wird und einen angemessenen Schutz Personenbezogener Daten bietet.

b) „**Verbundenes Unternehmen**“ bezeichnet in Bezug auf eine Partei jedes Unternehmen, das direkt oder indirekt die Kontrolle über diese Partei hat, unter deren Kontrolle steht oder mit einer solchen Partei unter gemeinsamer Kontrolle steht (aber nur so lange, wie eine solche Kontrolle besteht).

c) „**Anwendbare Datenschutzgesetze**“ bezeichnet alle Gesetze und Vorschriften, die für die Verarbeitung Personenbezogener Daten gemäß dem Hauptvertrag gelten, einschließlich der Europäischen Datenschutzgesetze und der CCPA.

d) „**CCPA**“ bezeichnet das California Consumer Privacy Act von 2018 (Cal. Civ. Code § 1798.100 - 1798.199, 2018).

e) „**Cloudflare Group**“ bezeichnet Cloudflare und alle mit ihr verbundenen Unternehmen.

f) „**Verantwortlicher**“ bezeichnet eine Einheit, die die Zwecke und Mittel der Verarbeitung Personenbezogener Daten festlegt.

g) „**Kundengruppe**“ bezeichnet den Kunden und alle verbundenen Unternehmen.

h) „**Europäische Datenschutzgesetze**“ bezeichnet alle Gesetze und Vorschriften der Europäischen Union, des Europäischen Wirtschaftsraums, ihrer Mitgliedstaaten, der Schweiz und des Vereinigten Königreichs, die für die Verarbeitung Personenbezogener Daten gemäß dem Hauptvertrag gelten (einschließlich gegebenenfalls (i) der Verordnung 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, wie sie gemäß Abschnitt 3 des Gesetzes von 2018 zum Austritt des Vereinigten Königsreiches aus der Europäischen Union festgehalten wurde (die **„UK-DSGVO**“); (iii) die EU e-Privacy-Richtlinie (Richtlinie 2002/58/EG); und (iv) jegliche nationalen Datenschutzgesetze, die gemäß, infolge von (i), (ii) oder (iii) erlassen oder im Zusammenhang mit (i), (ii) oder (iii) anwendbar sind.

i) „**Personenbezogene Daten**“ bezeichnet alle Daten, die im Rahmen des geltenden Datenschutzrechts als „Personenbezogene Daten“, „*Personenbezogene Informationen*“ oder „*Daten zur Identifizierung von Personen*“ (oder analoge Begriffe) definiert sind.

j) „**Verarbeitung**“, „**betroffene Person**“ und „**Aufsichtsbehörde**“ haben die Bedeutung, die ihnen im Europäischen Datenschutzrecht zugewiesen wird.

k) „**Auftragsverarbeiter**“ bezeichnet eine Stelle, die Personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet, einschließlich einer Stelle, an die eine andere Stelle gemäß einem schriftlichen Vertrag die Personenbezogenen Daten einer natürlichen Person für einen geschäftlichen Zweck offenlegt, welcher der die Informationen erhaltenden Stelle dazu verpflichtet, die Daten nur zum Zweck der Erbringung der Dienstleistungen zu speichern, zu verwenden oder offenzulegen.

l) „**Dienste**“ bezieht sich auf alle Cloud-basierten Lösungen, die von Cloudflare oder seinen autorisierten Partnern angeboten, vermarktet oder verkauft werden und die dazu bestimmt sind,die Leistung, Sicherheit und Verfügbarkeit von Internet-Eigenschaften, -Anwendungen und -Netzwerken zu erhöhen, zusammen mit jeglicher Software, Software Entwicklungssets und Anwendungsprogrammierschnittstellen ("**APIs**"), die in Verbindung mit dem Vorgenannten zur Verfügung gestellt werden.

m) „**SVK**“ bezeichnet: (i) in Fällen, in denen die EU-DSGVO oder das schweizerische Bundesgesetz über den Datenschutz gilt, die Vertragsklauseln im Anhang zum Durchführungsbeschluss 2021/914 vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung Personenbezogener Daten in Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates („**SVK der EU**“); und (ii) wenn die UK-DSGVO gilt, Standard-Datenschutzklauseln, die gemäß Artikel 46 der UK-DSGVO angenommen oder zulässig sind („**SVK des UK**“).

n) „**Beschränkte Übertragung**“ bezeichnet: (i) in Fällen, in denen die EU-DSGVO oder das schweizerische Bundesgesetz über den Datenschutz gilt, eine Übermittlung Personenbezogener Daten aus dem Europäischen Wirtschaftsraum oder der Schweiz (falls zutreffend) in ein Land außerhalb des Europäischen Wirtschaftsraums oder der Schweiz (falls zutreffend), das keinem Angemessenheitsbeschluss der Europäischen Kommission oder des Eidgenössischen Datenschutz-

und Öffentlichkeitsbeauftragten unterliegt (wie jeweils zutreffend); und (ii) sofern die UK-DSGVO gilt, eine Übermittlung Personenbezogener Daten aus dem Vereinigten Königreich in ein jedwedes anderes Land, die nicht auf Angemessenheitsbestimmungen gemäß § 17A des UK-Datenschutzgesetzes von 2018 beruht.

1.2 Ein Unternehmen übt „**eine Kontrolle**“ über ein anderes Unternehmen aus, wenn es: (a) die Mehrheit der Stimmrechte an ihm hält; (b) Gesellschafter oder Aktionär desselben ist und über das Recht verfügt, eine Mehrheit seines Leitungs- oder Verwaltungsorgans abzuberufen; (c) Gesellschafter oder Aktionär desselben ist und allein oder gemäß einer Vereinbarung mit anderen Aktionären oder Gesellschaftern die Mehrheit der Stimmrechte in diesem Unternehmen hält; oder (d) das Recht hat, aufgrund seiner Gründungsunterlagen oder aufgrund eines Vertrages einen beherrschenden Einfluss auf dieses Unternehmen auszuüben, und zwei Unternehmen werden als „**unter gemeinsamer Kontrolle**“ stehend behandelt, wenn eine das andere (direkt oder indirekt) beherrscht oder beide (direkt oder indirekt) von demselben Unternehmen beherrscht werden.

2. Rechtsstellung der Parteien

2.1 Art der Personenbezogenen Daten, die gemäß diesem NDV verarbeitet werden und Gegenstand, Dauer, Art und Zweck der Verarbeitung und die Kategorien der Betroffenen Personen werden in Anhang 1 beschrieben.

2.2 Jede Partei garantiert in Bezug auf Personenbezogene Daten, dass sie die geltenden Datenschutzgesetze einhalten wird. Das Verhältnis zwischen den Parteien betreffend haftet der Kunde allein für die Richtigkeit, Qualität und Rechtmäßigkeit der Personenbezogenen Daten und die Mittel, mit denen der Kunde Personenbezogene Daten erworben hat.

2.3 In Bezug auf die Rechte und Pflichten der Parteien aus diesem NDV in Bezug auf die Personenbezogenen Daten erkennen die Parteien an und vereinbaren, dass der Kunde der Verantwortliche (oder ein Auftragsverarbeiter, der Personenbezogene Daten im Auftrag eines Dritt-Verantwortlichen verarbeitet) ist und Cloudflare Auftragsverarbeiter (oder gegebenenfalls Unterauftragsverarbeiter) ist.

2.4 Wenn der Kunde Auftragsverarbeiter ist, garantiert der Kunde der Cloudflare, dass die Anweisungen und Handlungen des Kunden in Bezug auf die Personenbezogenen Daten, einschließlich der Benennung von Cloudflare als anderer Auftragsverarbeiter und, sofern zutreffend, der Abschluss der SVK von dem entsprechenden Dritt-Verantwortlichen genehmigt wurden (und für die Dauer dieses NDV weiterhin werden).

3. Verpflichtungen von Cloudflare

3.1 In Bezug auf alle Personenbezogenen Daten, die sie als Auftragsverarbeiter oder Unterauftragsverarbeiter verarbeitet, garantiert Cloudflare:

(a) Personenbezogene Daten nur zu verarbeiten, um den Dienst zu erbringen und in Übereinstimmung mit: (i) den schriftlichen Anweisungen des Kunden, wie im Hauptvertrag und diesem NDV festgelegt, es sei denn, Cloudflare ist nach geltendem Unionsrecht oder dem Recht der Mitgliedstaaten dazu verpflichtet, und (ii) den Anforderungen der geltenden Datenschutzgesetze. Falls Cloudflare verpflichtet ist, personenbezogene Daten gemäß den anwendbaren Datenschutzgesetzen zu verarbeiten, informiert Cloudflare den Kunden vor der Verarbeitung über diese gesetzliche Verpflichtung, es sei denn, das Gesetz verbietet eine solche Information aus wichtigen Gründen des öffentlichen Interesses;

(b) die Personenbezogenen Daten nicht für andere Zwecke als für den spezifischen Zweck der Erbringung des Dienstes zu verkaufen, zu speichern, zu verwenden oder weiterzugeben, einschließlich zu einem anderen kommerziellen Zweck als der Erbringung des Dienstes. Cloudflare darf die Personenbezogenen Daten nicht zu Marketing- oder Werbezwecken verwenden. Die Erbringung der Dienste durch Cloudflare kann die Offenlegung Personenbezogener Daten an Unterauftragsverarbeiter einschließen, wenn dies in Übereinstimmung mit Abschnitt 4 dieses NDV geschieht;

(c) den Kunden zu informieren, wenn nach Ansicht von Cloudflare die vom Kunden unter Klausel 3.1(a) bereitgestellten Anweisungen gegen geltende Datenschutzgesetze verstoßen;

(d) geeignete technische und organisatorische Maßnahmen zu implementieren, um sicherzustellen, dass ein den Risiken, die die Verarbeitung Personenbezogener Daten birgt, angemessenes Schutzniveau geboten ist, insbesondere was den Schutz vor unbeabsichtigter oder unrechtmäßiger Zerstörung, Verlust, Veränderung, unbefugter Weitergabe oder unberechtigtem Zugriff auf Personenbezogene Daten anbetrifft. Solche Maßnahmen umfassen, ohne Einschränkungen, insbesondere die in Anhang 2 genannten Sicherheitsmaßnahmen („**Sicherheitsmaßnahmen**"). Der Kunde erkennt an, dass die Sicherheitsmaßnahmen dem technischen Fortschritt und der Entwicklung unterliegen und dass Cloudflare die Sicherheitsmaßnahmen von Zeit zu Zeit aktualisieren oder ändern kann, vorausgesetzt, dass diese Aktualisierungen und Änderungen die Gesamtsicherheit des Dienstes nicht beeinträchtigen oder mindern;

(e) sicher zu stellen, dass nur autorisiertes Personal Zugang zu diesen Personenbezogenen Daten hat und dass jede Person, die sie berechtigt, Zugriff auf die Personenbezogenen Daten zu erhalten, einer vertraglichen oder gesetzlichen Geheimhaltungspflicht unterliegt;

(f) unverzüglich den Kunden bei Kenntnis über Sicherheitsverletzungen zu informieren, die zur versehentlichen oder unrechtmäßigen Zerstörung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung oder zum Zugriff auf Personenbezogene Daten führt, die zum Zwecke der Bereitstellung der Dienste durch Cloudflare, dessen Unterauftragnehmer oder andere identifizierte oder nicht identifizierbare Dritte an den Kunden, übermittelt, gespeichert oder anderweitig verarbeitet werden („**Verletzung des Schutzes Personenbezogener Daten**") und dem Kunden eine angemessene Zusammenarbeit und Unterstützung in Bezug auf diese Verletzung des Schutzes Personenbezogener Daten zu gewähren, einschließlich aller angemessenen Informationen im Besitz von Cloudflare in Bezug auf diese Verletzung des Schutzes Personenbezogener Daten, soweit sie die Personenbezogenen Daten beeinträchtigen;

(g) ohne die vorherige schriftliche Zustimmung des Kunden keine öffentliche Bekanntmachung über eine Verletzung des Schutzes Personenbezogener Daten (eine „**Verletzungsmitteilung**") abzugeben, es sei denn, dies ist nach geltendem Recht vorgeschrieben;

(h) soweit Cloudflare in der Lage ist, zu überprüfen, ob eine betroffene Person mit dem Kunden verbunden ist, den Kunden unverzüglich zu informieren, wenn sie eine Anfrage einer betroffenen Person auf Ausübung von Datenschutzrechten erhält (einschließlich dem Recht auf Auskunft, Berichtigung oder Löschung) in Bezug auf die Personenbezogenen Daten dieser betroffenen Person (eine „**Anfrage der betroffenen Person**"). Cloudflare wird nicht ohne vorherige schriftliche Zustimmung des Kunden die Anfrage der betroffenen Person beantworten, es sei denn, um zu bestätigen, dass diese Anfrage den Kunden betrifft, womit sich der Kunde hiermit einverstanden erklärt;

(i) soweit Cloudflare in der Lage ist, und im Einklang mit geltendem Recht, dem Kunden bei der Beantwortung der Anfrage einer betroffenen Person hinsichtlich der Ausübung ihrer

Datenschutzrechte (einschließlich des Rechts auf Auskunft, Berichtigung oder Löschung) bezüglich der Personenbezogenen Daten der betroffenen Person angemessene Unterstützung zu leisten, wenn der Kunde nicht die Möglichkeit hat, eine Anfrage der betroffenen Person ohne Unterstützung von Cloudflare zu beantworten. Der Kunde ist dafür verantwortlich, zu überprüfen, dass der Antragsteller die betroffene Person ist, deren Personenbezogenen Daten von der Anfrage betroffen sind. Cloudflare trägt keine Verantwortung für die dem Kunden unter Berufung auf diesen Unterabschnitt in redlicher Absicht bereitgestellten Informationen. Der Kunde trägt alle Kosten, die Cloudflare im Zusammenhang mit der Bereitstellung dieser Unterstützung entstehen;

(j) abgesehen von dem Umfang, der für die Einhaltung des geltenden Rechts erforderlich ist, nach Beendigung oder Ablauf des Hauptvertrages oder abgeschlossenen Erbringung des Dienstes nach Wahl des Kunden alle Personenbezogenen Daten (einschließlich Kopien davon), die gemäß diesem NDV verarbeitet werden, zu löschen oder zurückzugeben;

(k) unter Berücksichtigung der Art der Verarbeitung und der Informationen, die Cloudflare zur Verfügung stehen, dem Kunden Unterstützung zu gewähren, wenn dieser eine solche Unterstützung gemäß den Verpflichtungen von Cloudflare im Rahmen der geltenden Datenschutzgesetze anfordert, und zwar in Bezug auf:

(i) Datenschutz-Folgenabschätzungen und vorherige Konsultationen (wie diese Begriffe in den geltenden Datenschutzgesetzen definiert sind);

(ii) Mitteilungen an die Aufsichtsbehörde nach geltendem Datenschutzrecht und/oder Mitteilungen an betroffene Personen durch den Kunden als Reaktion auf einen Verstoß gegen den Schutz Personenbezogener Daten; und

(iii) die Einhaltung seiner Pflichten aus geltendem Datenschutzrecht in Bezug auf die Sicherheit der Verarbeitung;

unter der Voraussetzung, dass der Kunde alle Kosten übernimmt, die Cloudflare im Zusammenhang mit der Erbringung dieser Unterstützung entstehen.

4. Vergabe von Unteraufträgen

4.1 Cloudflare gibt Personenbezogene Daten nur für die Zwecke der Erbringung der Dienstleistungen an Unterauftragsverarbeiter weiter. Cloudflare verkauft oder gibt Personenbezogene Daten nicht zu kommerziellen Zwecken an Dritte weiter.

4.2 Der Kunde erteilt eine allgemeine schriftliche Vollmacht: (a) an Cloudflare zur Bestellung weiterer Mitglieder der Cloudflare-Gruppe als Unterauftragsverarbeiter und (b) an Cloudflare und andere Mitglieder der Cloudflare-Gruppe zur Bestellung externer Rechenzentren und Business-, Engineering- und Kundensupportanbietern, um die Leistung des Services zu unterstützen.

4.3 Cloudflare führt eine Liste von Unterauftragsverarbeitern unter https://www.cloudflare.com/gdpr/subprocessors/ und wird die Namen neuer und ersetzender Unterauftragsverarbeiter in die Liste mindestens dreißig (30) Tage vor dem Datum, an dem diese Unterauftragsverarbeiter mit der Verarbeitung Personenbezogener Daten beginnen, in die Liste einfügen. Widerspricht der Kunde einem neuen oder Ersatz-Unterauftragsverarbeiter aus angemessenen Gründen im Zusammenhang mit dem Datenschutz, so teilt er diese Einwände innerhalb von zehn (10) Tagen nach der Benachrichtigung schriftlich mit, und die Parteien bemühen sich, diese Angelegenheit nach Treu und Glauben zu klären. Wenn Cloudflare vernünftigerweise in der Lage ist, den Service gemäß Hauptvertrag zu erbringen, ohne den Unterauftragsverarbeiter zu nutzen und nach eigenem Ermessen so entscheidet, hat der Kunde keine weiteren Rechte gemäß dieser Klausel 4.3 in Bezug auf die vorgeschlagene Nutzung

des Unterauftragsverarbeiters. Wenn Cloudflare nach eigenem Ermessen die Nutzung des Unterauftragsverarbeiters verlangt und nicht in der Lage ist, den Einwand des Kunden bei der geplanten Verwendung des neuen oder Ersatz-Unterauftragsverarbeiters zu befriedigen, kann der Kunde das betreffende Bestellformular mit Wirkung ab dem Datum kündigen, an dem Cloudflare mit der Nutzung dieses neuen oder Ersatz-Unterauftragsverarbeiters beginnt und zwar ausschließlich in Bezug auf den/die Dienste(e), für den/die der vorgeschlagene neue Unterauftragsverarbeiter zur Verarbeitung Personenbezogener Daten verwendet wird. Erhebt der Kunde nicht rechtzeitig Widerspruch gegen einen neuen oder Ersatz-Unterauftragsverarbeiter gemäß dieser Klausel 4.3, so wird davon ausgegangen, dass der Kunde dem Unterauftragsverarbeiter zugestimmt hat und auf sein Widerspruchsrecht verzichtet.

4.4 Cloudflare stellt sicher, dass jeder Unterauftragsverarbeiter, den sie mit der Erbringung eines Aspekts des Dienstes in ihrem Namen in Verbindung mit diesem NDV beauftragt, dies nur auf Grundlage eines schriftlichen Vertrags tut, der diesem Unterauftragsverarbeiter Bedingungen auferlegt (z.B. Pflichten im Bereich des Datenschutzes), die den Schutz Personenbezogener Daten nicht weniger gewährleisten als die Cloudflare in diesem NDV auferlegt sind (die "**Einschlägigen Bedingungen").** Cloudflare sorgt für die Einhaltung der einschlägigen Bedingungen durch diesen Unterauftragsverarbeiter und haftet gegenüber dem Kunden für jede Verletzung einer der einschlägigen Bedingungen durch diesen Unterauftragsverarbeiter.

5. Audit und Aufzeichnungen

5.1 Cloudflare stellt dem Kunden in Übereinstimmung mit den anwendbaren Datenschutzgesetzen die Informationen zur Verfügung, die sich im Besitz oder unter der Kontrolle von Cloudflare befinden und die der Kunde in angemessener Weise anfordern kann, um nachzuweisen, dass Cloudflare die Verpflichtungen von Auftragsverarbeitern gemäß den anwendbaren Datenschutzgesetzen in Bezug auf die Verarbeitung Personenbezogener Daten erfüllt.

5.2 Cloudflare kann das Recht des Kunden auf Durchführung eines Audits nach geltendem Datenschutzrecht erfüllen, indem folgendes vorgelegt wird:

(a) ein Prüfbericht, der nicht älter als dreizehn (13) Monate ist, erstellt durch einen unabhängigen externen Prüfer, der belegt, dass die technischen und organisatorischen Maßnahmen von Cloudflare ausreichend sind und in Übereinstimmung mit einem anerkannten Standard für die Prüfung in der Branche erfüllt sind;

(b) zusätzliche Informationen, die sich im Besitz oder unter der Kontrolle von Cloudflare befinden, eine Datenschutzaufsichtsbehörde auf Anforderung oder zur notwendigen Bereitstellung zusätzlicher Informationen in Bezug auf die Verarbeitung Personenbezogener Daten, die Cloudflare im Rahmen dieses NDV durchführt, und

(c) soweit die Personenbezogenen Daten des Kunden den SVK unterliegen und die gemäß dieser Klausel 5.2 zur Verfügung gestellten Informationen nach vernünftigem Ermessen des Kunden nicht ausreichen, um die Einhaltung ihrer Verpflichtungen aus diesem NDV oder den geltenden Datenschutzgesetzen nachzuweisen, wird Cloudflare es dem Kunden ermöglichen, einmal jährlich während der Laufzeit (wie im Hauptvertrag definiert) ein Vor-Ort-Audit anzufordern, um zu überprüfen, ob Cloudflare ihre Verpflichtungen aus diesem NDV gemäß Klausel 5.3 erfüllt.

5.3 Für die Anforderung eines Audits durch den Kunden gelten folgende zusätzliche Bedingungen:

(a) Der Kunde hat alle Anträge auf Überprüfung der Auditberichte von Cloudflare an compliance@cloudflare.com zu richten.

(b) Nach Eingang einer Auditanfrage bei Cloudflare gemäß Klausel 5.2 Buchstabe c, werden Cloudflare und der Kunde vorab das angemessene Anfangsdatum, den Umfang, die Dauer und die Kontrollen

von Sicherheit und Vertraulichkeit gemäß Klausel 5.2 Buchstabe c erörtern und vereinbaren. Wenn möglich, sind die Beweise für eine solche Prüfung auf die für die jüngste Prüfung von Cloudflare gesammelten Beweismittel beschränkt.

(c) Cloudflare kann für jede Prüfung gemäß Klausel 5.2 Buchstabe c eine Gebühr (auf der Grundlage der angemessenen Kosten von Cloudflare) in Rechnung stellen. Cloudflare stellt dem Kunden vor einer solchen Prüfung weitere Einzelheiten zu etwaigen Gebühren und Berechnungsgrundlagen zur Verfügung. Der Kunde ist für alle Gebühren verantwortlich, die von einem vom Kunden beauftragten Prüfer für die Durchführung einer solchen Prüfung in Rechnung gestellt werden.

(d) Cloudflare kann einem vom Kunden mit der Durchführung einer Prüfung gemäß Klausel 5.2(c) ernannten Wirtschaftsprüfer schriftlich widersprechen, wenn der Wirtschaftsprüfer nach billigem Ermessen von Cloudflare nicht angemessen qualifiziert oder nicht unabhängig ist, ein Wettbewerber von Cloudflare oder anderweitig offensichtlich ungeeignet ist (d.h. ein Prüfer, dessen Beauftragung eine mit den vorgenannten Aspekten vergleichbare schädliche Auswirkung auf das Geschäft von Cloudflare haben kann). Ein solcher Einwand durch Cloudflare erfordert vom Kunden, einen anderen Prüfer zu bestellen oder die Prüfung selbst durchzuführen. Sofern die SVK Anwendung finden, ändert oder modifiziert diese Klausel 5.3 weder die SVK, noch die Rechte der Aufsichtsbehörde oder der betroffenen Person im Rahmen der SVK.

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

6.1 Im Zusammenhang mit dem Dienst gehen die Parteien davon aus, dass Cloudflare (und deren Unterauftragsverarbeiter) bestimmte Personenbezogene Daten, die durch die Europäischen Datenschutzgesetze geschützt sind, für die der Kunde oder ein Mitglied der Kundengruppe ein Verantwortlicher (oder ein Auftragsverarbeiter im Auftrag eines Dritt-Verantwortlichen sein kann, falls zutreffend) außerhalb des Europäischen Wirtschaftsraums („**EWR**“), der Schweiz und dem Vereinigten Königreich verarbeiten können.

6.2 Die Parteien vereinbaren, dass, wenn die Übertragung durch die Europäischen Datenschutzgesetze geschützter Personenbezogener Daten vom Kunden oder einem Mitglied der Kundengruppe an Cloudflare eine eingeschränkte Übertragung ist, diese, wie folgt, den entsprechenden SVK unterliegt:

(a) in Bezug auf Personenbezogene Daten, die durch die EU-DSGVO geschützt sind, gelten die SVK der EU wie folgt:

(i) Modul Zwei findet Anwendung, wenn der Kunde (oder das jeweilige Mitglied der Kundengruppe) ein Verantwortlicher ist und Modul Drei findet Anwendung, wenn der Kunde (oder das jeweilige Mitglied der Kundengruppe) Auftragsverarbeiter ist;

(ii) unter Klausel 7 gilt die optionale Docking-Klausel;

(iii) unter Klausel 9 gilt die Option 2 und die Frist für die vorherige Mitteilung der Änderungen des Unterauftragsverarbeiters richtet sich nach Klausel 4.3 dieses NDV;

(iv) unter Klausel 11 gilt die optionale Sprache nicht;

(v) in Klausel 17 findet die Option 2 Anwendung und wenn der Mitgliedstaat des Datenexporteurs keine Rechte für Drittbegünstigte zulässt, dann gilt das deutsche Recht;

(vi) in Klausel 18 Buchstabe b werden Streitigkeiten den Gerichten der Gerichtsbarkeit, die den Hauptvertrag zwischen den Parteien regeln, unterworfen oder, wenn es sich bei

diesen Gerichtsbarkeiten nicht um einen EU-Mitgliedstaat handelt, den Gerichten in München, Deutschland. In jedem Fall sind die Klauseln 17 und 18 Buchstabe b dahingehend konsequent, dass die Wahl des Gerichtsstands und der Zuständigkeit auf das Land des geltenden Rechts fällt;

(vii) Anlage I der SVK der EU gilt als durch die in Anhang 1 zu diesen NDV aufgeführten Informationen ergänzt; und

(viii) Anhang II der SVK der EU gilt als durch die in Anhang 2 zu diesem NDV aufgeführten Informationen ergänzt;

(b) in Bezug auf Personenbezogene Daten, die durch die UK-DSGVO geschützt sind, gelten die SVK der EU wie folgt:

(i) Solange es rechtmäßig zulässig ist, sich für die Übertragung Personenbezogener Daten an Auftragsverarbeiter auf die Standardvertragsklauseln zu stützen, die im Beschluss der Europäischen Kommission vom 5. Februar 2010 („**vormals C2P SVK**“) für die Übermittlung Personenbezogener Daten aus dem Vereinigten Königreich festgelegt sind, gelten die Prior C2P SVK zwischen dem Kunden (oder dem jeweiligen Mitglied der Kundengruppe) und Cloudflare auf folgender Grundlage:

(A) Die Anlage 1 ist durch die einschlägigen Informationen in Anhang 1 dieses NDV zu ergänzen;

(B) Die Anlage 2 ist durch die einschlägigen Informationen in Anhang 2 dieses NDV zu ergänzen;

(C) die optionale, veranschaulichende Entschädigungsklausel findet keine Anwendung.

(ii) Wenn die obige Unterklausel (b)(i) keine Anwendung findet, der Kunde (oder das jeweilige Mitglied der Kundengruppe) und Cloudflare jedoch gesetzlich berechtigt sind, sich für die Übermittlung Personenbezogener Daten aus dem Vereinigten Königreich, vorbehaltlich des Abschlusses des „UK-Nachtrags zu den EU-Standardvertragsklauseln“ („**UK-Nachtrag**“**)** auf die SVK der EU zu stützen, das vom Amt des Informationsbeauftragten gemäß s.119A Absatz 1 des Datenschutzgesetzes 2018 erstellt wurde, dann:

(A) Die gemäß Abschnitt 6.2 Buchstabe a dieses NDV ausgefüllten SVK der EU gelten auch für die Übermittlung dieser Personenbezogenen Daten vorbehaltlich der nachstehenden Unterklausel (B);

(B) Der Nachtrag zum Vereinigten Königreich gilt als zwischen dem übertragenden Kunden (oder dem jeweiligen Mitglied der Kundengruppe) und Cloudflare abgeschlossen, und die SVK der EU gelten als durch den britischen Nachtrag hinsichtlich der Übertragung dieser Personenbezogenen Daten als geändert.

(iii) Findet weder die Unterklausel (b)(i), noch die Unterklausel (b)(ii) Anwendung, dann bemühen sich der Kunde und Cloudflare unverzüglich gemeinsam nach Treu und Glauben, geeignete Schutzmaßnahmen für die Übermittlung dieser Personenbezogenen Daten zu treffen, die gemäß UK-DSGVO erforderlich oder zulässig sind.

(c) in Bezug auf Personenbezogene Daten, die durch das Schweizerische Bundesgesetz über den Datenschutz (in der jeweils geänderten oder ersetzten Fassung) geschützt sind, gelten die gemäß Klausel 6.2 Buchstabe a dieses NDV ergänzten SVK der EU für die Übermittlung solcher Personenbezogenen Daten, es sei denn,

(i) für diese Personenbezogenen Daten ist die zuständige Aufsichtsbehörde der Eidgenössische Datenschutz- und Informationsbeauftragte;

(ii) in Klausel 17 ist das anwendbare Recht das Recht der Schweiz;

(iii) Bezugnahmen auf „Mitgliedstaat(en)" in den SVK der EU werden so ausgelegt, dass sie sich auf die Schweiz beziehen, und betroffene Personen mit Sitz in der Schweiz sind berechtigt, ihre Rechte aus den EU SVK in der Schweiz auszuüben und durchzusetzen; und

(iv) Verweise auf die „Datenschutz-Grundverordnung", „Verordnung 2016/679" oder „DSGVO" in den SVK sind Bezugnahmen auf das Schweizerische Bundesgesetz über den Datenschutz (in der jeweils geänderten oder ersetzten Fassung).

(d) für die SVK gelten folgende Bedingungen:

(i) Der Kunde kann sein in Klausel 5 dieses NDV festgelegtes Auditrecht im Rahmen der SVK ausüben; und

(ii) Cloudflare kann Unterauftragsverarbeiter gemäß den Bestimmungen in und vorbehaltlich der Anforderungen der Klauseln 4 und 6.3 dieses NDV benennen, und der Kunde kann sein Recht ausüben, Unterauftragsverarbeitern unter den SVK in der in Abschnitt 4.3 dieses NDV dargelegten Weise zu widersprechen; und

(e) steht eine Bestimmung dieses NDV unmittelbar oder mittelbar gegen die SVK im Widerspruch, so haben die SVK Vorrang.

6.3 In Bezug auf eingeschränkte Übermittlungen an Cloudflare gemäß Abschnitt 6.2 beteiligt sich Cloudflare nicht (und gestattet dies keinem Unterauftragsverarbeiter) an weiteren eingeschränkten Übermittlungen Personenbezogener Daten (gleichgültig, ob als „Exporteur" oder als „Importeur" der Personenbezogenen Daten), es sei denn, diese weitere eingeschränkte Übermittlung erfolgt in voller Übereinstimmung mit den Europäischen Datenschutzgesetzen und gemäß den SVK, die zwischen dem Exporteur und Importeur der Personenbezogenen Daten implementiert wurden oder es gilt ein alternativer Transfermechanismus (wie in Klausel 6.5 definiert), der vom Importeur angenommen wurde.

6.4 Falls der Kunde versucht, eine Bewertung der Angemessenheit der SVK für Übermittlungen in bestimmte Länder oder Regionen vorzunehmen, wird Cloudflare, soweit sie in der Lage ist, dem Kunden im Rahmen einer solchen Beurteilung angemessene Unterstützung leisten, vorausgesetzt, der Kunde trägt alle Kosten, die Cloudflare im Zusammenhang mit der Erbringung einer solchen Unterstützung entstehen.

6.5 Soweit Cloudflare einen alternativen Datenübermittlungsmechanismus (einschließlich einer neuen Version oder Folgeversion eines Privacy Shields, das gemäß den geltenden Europäischen Datenschutzgesetzen angenommen wurde) für die nicht in diesem NDV beschriebene Übertragung von Personenbezogenen Daten einführt („**Alternativer Datenübermittlungsmechanismus**"), gilt anstelle eines in diesem NDV beschriebenen Übermittlungsmechanismus (jedoch nur insoweit dieser alternative

Übermittlungsmechanismus dem Europäischen Datenschutzrecht entspricht und sich auf die Gebiete erstreckt, in die Personenbezogene Daten übertragen werden) der alternative Datenübermittlungsmechanismus, und der Kunde stimmt zu, andere und weitere Dokumente zu unterzeichnen und andere und weitere Maßnahmen zu ergreifen, die vernünftigerweise notwendig sein können, um diesem alternativen Datenübermittlungsmechanismus eine rechtliche Wirksamkeit zu verleihen.

7. Zugriffsanfragen Dritter

7.1 Wenn Cloudflare Kenntnis von einem Rechtsverfahren Dritter erlangt, das Personenbezogene Daten anfordert, die Cloudflare im Namen des Kunden in seiner Rolle als Auftragsverarbeiter oder Unterauftragsverarbeiter (wie jeweils zutreffend) verarbeitet, wird Cloudflare:

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

(b) den Dritten darüber informieren, dass sie ein Auftragsverarbeiter oder Unterauftragsverarbeiter (wie jeweils zutreffend) der Personenbezogenen Daten ist und nicht ohne die Zustimmung des Kunden zur Offenlegung der Personenbezogenen Daten berechtigt ist;

(c) dem Dritten die erforderlichen Mindestangaben der Kontaktdaten des Kunden offenlegen, damit der Dritte sich an den Kunden wenden kann und den Dritten anweisen, seine Datenanfrage an den Kunden zu richten; und

(d) soweit Cloudflare Zugang zu Personenbezogenen Daten gibt oder diese im Rahmen eines rechtlichen Verfahrens Dritter entweder mit der Einwilligung des Kunden oder aufgrund einer zwingenden rechtlichen Verpflichtung offenlegt, wird Cloudflare das Mindestmaß an Personenbezogenen Daten offenlegen, soweit dies gesetzlich vorgeschrieben und in Übereinstimmung mit dem anwendbaren rechtlichen Verfahren ist.

7.2 In ihrer Eigenschaft als Auftragsverarbeiter oder Unterauftragsverarbeiter kann Cloudflare gegebenenfalls dem von einer Regierungsbehörde (einschließlich einer Justizbehörde) eingeleiteten rechtlichen Verfahren Dritter unterliegen bei dem der Zugang zu oder die Offenlegung von Personenbezogenen Daten verlangt wird. Wenn Cloudflare Kenntnis eines jedweden rechtlichen Verfahrens Dritter erhält, das von einer Regierungsbehörde (einschließlich einer Justizbehörde) veranlasst wurde und in dem Personenbezogene Daten angefordert werden, die Cloudflare im Namen des Kunden in ihrer Eigenschaft als Auftragsverarbeiter oder Unterauftragsverarbeiter (wie jeweils zutreffend) verarbeitet, dann wird Cloudflare in dem Maße, in dem Cloudflare die Aufforderung mit einem angemessen Aufwand prüft und infolgedessen in der Lage ist feststellen zu können, dass dieses rechtliche Verfahren Dritter, die Personenbezogene Daten anfordern, eine Gesetzeskollision zur Folge hat:

(a) alle in vorstehender Klausel 7.1 genannten Maßnahmen ergreifen;

(b) sich alle Rechtsbehelfe vorbehalten, bevor sie Personenbezogene Daten in einem Prozess bis zur Berufungsgerichtsebene vorlegt; und

(c) Personenbezogene Daten erst dann offenlegen (und dann nur in dem Umfang), wie dies nach den geltenden verfahrensrechtlichen Vorschriften erforderlich ist.

7.3 Die Klauseln 7.1 und 7.2 finden keine Anwendung, wenn Cloudflare nach gutem Glauben annimmt, dass die Aufforderung der Regierung aufgrund eines Notfalls, der wegen der Todesgefahr oder einer schweren körperlichen Verletzung einer Person erforderlich ist. In einem solchen Fall wird Cloudflare den Kunden so schnell wie möglich nach der Offenlegung über die Offenlegung informieren und dem

Kunden sämtliche diesbezügliche Informationen mitteilen, es sei denn, eine solche Offenlegung ist rechtlich untersagt.

7.4 Cloudflare stellt dem Kunden regelmäßig Informationen über rechtliche Verfahren Dritter, die Personenbezogene Daten anfordern, in Form des halbjährlichen Transparenzberichts von Cloudflare, der unter https://www.cloudflare.com/transparency/ abrufbar ist.

7.5 Ab dem Datum, an dem der Kunde dieses NDV mit Cloudflare abgeschlossen hat, geht Cloudflare die nachstehend aufgeführten Verpflichtungen ein. Cloudflare aktualisiert erforderlichenfalls diese Verpflichtungen gemäß der Anforderungen unter https://www.cloudflare.com/transparency/https://www.cloudflare.com/transparency/:

(a) Cloudflare hat unsere Verschlüsselungs- oder Authentifizierungsschlüssel oder die Verschlüsselungs- oder Authentifizierungsschlüssel unserer Kunden niemals an Dritte weitergegeben.

(b) Cloudflare hat niemals irgendeine Strafverfolgungssoftware oder -ausrüstung in unserem Netzwerk installiert.

(c) Cloudflare hat niemals einer Strafverfolgungsbehörde eine Eingabe der Inhalte unserer Kunden zu Verfügung gestellt, die unser Netzwerk durchqueren.

(d) Cloudflare hat niemals auf Verlangen von Strafverfolgungsbehörden oder anderen Dritten ihre Verschlüsselung geschwächt, beeinträchtigt oder umgeleitet.

8. Allgemeines

8.1 Dieser NDV berührt nicht die Rechte und Pflichten der Parteien aus dem Hauptvertrag, die weiterhin vollständig in Kraft bleiben. Im Falle eines Konflikts zwischen den Bedingungen dieses NDV und den Bestimmungen des Hauptvertrages haben die Bedingungen dieses NDV Vorrang, sofern der Gegenstand die Verarbeitung Personenbezogener Daten betrifft.

8.2 Die Haftung von Cloudflare im Rahmen oder in Verbindung mit diesem NDV, auch im Rahmen der SVK, unterliegt den im Hauptvertrag enthaltenen Haftungsausschlüssen und -beschränkungen. In keinem Fall beschränkt Cloudflare ihre Haftung gegenüber betroffenen Personen oder zuständigen Datenschutzbehörden bzw. schießt eine solche Haftung aus.

8.3 Außer wenn und sofern dies ausdrücklich in den SVK vorgesehen oder als Maßgabe des geltenden Datenschutzrechts erforderlich ist, verleiht dieser NDV keine Rechte Dritte; er ist nur zugunsten der Parteien und deren jeweils zulässigen Rechtsnachfolger und Abtretungsempfänger gedacht und darf nicht zugunsten einer anderen Person geltend gemacht werden.

8.4 Dieser NDV und alle damit verbundenen Handlungen unterliegen dem im Hauptvertrag bestimmten Recht, ohne dass dies zu Gesetzeskollisionen führt. Die Parteien stimmen der persönlichen Zuständigkeit dem Gerichtsstand der im Hauptvertrag festgelegten Gerichte zu.

8.5 Falls eine Bestimmung dieses NDV aus irgendeinem Grund für ungültig oder nicht durchsetzbar gehalten wird, bleiben die anderen Bestimmungen des NDV durchsetzbar. Ohne die Allgemeingültigkeit des Vorstehenden einzuschränken, erklärt sich der Kunde damit einverstanden, dass Klausel 8.2 (Haftungsbeschränkung) ungeachtet der Undurchführbarkeit jedweder anderer Bestimmung dieses NDV wirksam bleibt.

8.6 Dieser NDV ist die endgültige, vollständige und ausschließliche Vereinbarung der Parteien in Bezug auf den Vertragsgegenstand und ersetzt alle vorherigen Gespräche und Vereinbarungen zwischen den Parteien in Bezug auf diesen Gegenstand.

Anhang 1

Beschreibung der Datenverarbeitung

Dieser Anhang 1 ist Teil des NDV und beschreibt die Verarbeitung, die Cloudflare für den Kunden erbringt.

A. LISTE DER PARTEIEN

Datenexporteur(e): *Der Kunde muss die rechte Spalte ausfüllen.*

1.	Name: *Kunde und jedwede im Hauptvertrag beschriebene verbundene Unternehmen des Kunden.*	Wie im Hauptvertrag angegeben
	Adresse: *Adressen des Kunden und aller im Hauptvertrag beschriebenen verbundenen Unternehmen des Kunden. (oder anderweitig vom Kunden gegenüber Cloudflare mitgeteilt)*	Wie im Hauptvertrag angegeben
	Name, Funktion und Kontaktangaben des Ansprechpartners:	Wie im Hauptvertrag angegeben
	Aktivitäten, die für die im Rahmen dieses NDV und SVK übertragenen Daten relevant sind:	Nutzung des Dienstes gemäß dem Hauptvertrag.
	Unterschrift und Datum:	Dieser Anhang 1 gilt mit Unterzeichnung des NDV als wirksam.
	Funktion (Verantwortlicher/Auftragsverarbeiter):	Verantwortlicher (oder Auftragsverarbeiter im Auftrag eines Dritt-Verantwortlichen).

Datenimporteur(e):

1.	Name:	Cloudflare, Inc.
	Adresse:	101 Townsend Street San Francisco, CA 94107 USA
	Name, Funktion und Kontaktangaben des Ansprechpartners:	Emily Hancock Data Protection Officer legal@cloudflare.com
	Aktivitäten, die für die im Rahmen dieses NDV und SVK übertragenen Daten relevant sind:	Verarbeitung, die erforderlich ist, um dem Kunden den Dienst gemäß dem Hauptvertrag zu erbringen.

	Unterschrift und Datum:	Dieser Anhang 1 gilt mit Unterzeichnung des NDV als wirksam.
	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 („API“) und Anwendungen des Kunden zugreifen oder diese nutzen, oder (ii) Mitarbeiter, Vertreter oder Auftragnehmer des Kunden, die auf die Dienste zugreifen oder nutzen, wie z. B. Cloudflare Zero Trust Endnutzer, (zusammen „Endnutzer“). Natürliche Personen mit Anmeldedaten für ein Cloudflare-Konto und/oder Personen, die Dienstleistungen für einen Kunden verwalten („Administratoren“).
Kategorien der übertragenen Personenbezogenen Daten:	In Bezug auf Endnutzer: ● Alle Personenbezogenen Daten, die in Kundendatenprotokollen verarbeitet werden, wie IP-Adressen, und im Falle von Cloudflare Zero Trust, die Cloudflare Zero Trust End-nutzernamen und E-Mail-Adressen. „Kundenlogs“ bezeichnet alle Protokolle der Interaktionen von Endnutzern mit den Internet-Eigenschaften des Kunden und dem Service, die dem Kunden über das Service-Dashboard oder eine andere Online-Schnittstelle während der Laufzeit von Cloudflare zur Verfügung gestellt werden. ● Alle Personenbezogenen Daten, die in Kundeninhalten verarbeitet werden, dessen Umfang vom Kunden nach eigenem Ermessen bestimmt und gesteuert wird. „Kundeninhalte“ sind alle Dateien, Software, Skripten, Multimediabilder, Grafiken, Audio-, Video-, Text-, Daten- oder andere Objekte, die von Internet-Objekten , die dem Kunden gehören, kontrolliert oder vom Kunden betrieben oder vom Kunden über den Service hochgeladen, übertragen, verarbeitet und/oder in das Netzwerk von Cloudflare oder auf andere Weise über den Service vom Kunden

	übertragen, weitergeleitet und/oder zwischengespeichert werden. In Bezug auf Verwaltungsbenutzer: ● Alle Personenbezogenen Daten, die in Verwaltungs-Benutzerprüfungsprotokollen verarbeitet werden, wie IP-Adressen und E-Mail-Adressen.
Übertragene sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Schutzmaßnahmen, die vollständig der Art der Daten und der damit verbundenen Risiken Rechnung tragen, wie zum Beispiel strenge Zweckbindungen, Zugriffsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die spezialisierte Schulung durchgeführt haben), Aufzeichnungen des Zugangs zu Daten, Beschränkungen für die Weiterleitung oder zusätzliche Sicherheitsmaßnahmen:	Kunde, seine Endnutzer, Administratoren und/oder andere Partner können Inhalte auf die Online-Objekte des Kunden hochladen, die möglicherweise spezielle Datenkategorien umfassen können, deren Umfang vom Kunden nach eigenem Ermessen bestimmt und kontrolliert wird. Zu diesen besonderen Kategorien von Daten gehören unter Umständen Informationen über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit und die Verarbeitung von Daten über die Gesundheit oder das Sexualleben einer Person. Alle dieser besonderen Kategorien von Daten sind durch die Anwendung der in Anhang 2 beschriebenen Sicherheitsmaßnahmen zu schützen.
Häufigkeit der Übertragung (z.B. ob die Daten einmalig oder fortlaufend übertragen werden):	Fortgeltung während der Laufzeit des Hauptvertrages.
Art der Verarbeitung:	Verarbeitung, die erforderlich ist, um den Kunden den Dienst gemäß dem Hauptvertrag zu erbringen.
Zweck(e) der Datenübermittlung und Weiterverarbeitung:	Für die Erbringung des Dienstes erforderliche Verarbeitung.
Den Zeitraum, für den die Personenbezogenen Daten gespeichert werden, oder, wenn dies nicht möglich ist, die Kriterien, die für die Festlegung dieses Zeitraums verwendet werden:	Bis frühestens (i) Ablauf/Kündigung des Hauptvertrages oder (ii) dem Datum, an dem die Verarbeitung für die Zwecke der Erfüllung ihrer Verpflichtungen aus dem Hauptvertrag nicht mehr erforderlich ist (soweit anwendbar).
Für Übertragungen an (Unter-) Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben:	Gegenstand, Art und Dauer der Verarbeitung sind in im Hauptvertrag festgelegt.

C. ZUSTÄNDIGE AUFSICHTSBEHÖRDE

Identifizierung der zuständigen Aufsichtsbehörde/en gemäß (z.B. gemäß Klausel 13 der SVK)	In Bezug auf die SVK der EU bezeichnet die zuständige Aufsichtsbehörde, die gemäß Klausel 13 der SVK der EU festgelegt wurde. In Bezug auf die SVK des UK bedeutet dies das UK Information Commissioner's Office.

Anhang 2

Technische und organisatorische Sicherheitsmaßnahmen

Cloudflare hat ein Informationssicherheitsprogramm gemäß ISO/IEC 27000 Standards eingerichtet und hält dieses aufrecht. Cloudflare's Sicherheitsprogramm umfasst:

Maßnahmen zur Verschlüsselung Personenbezogener Daten

Cloudflare implementiert die Verschlüsselung, um Personenbezogene Daten angemessen zu schützen, und zwar unter Verwendung von folgendem:

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

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

Cloudflare verbessert die Sicherheit der Verarbeitungssysteme und Dienstleistungen in den Produktionsumgebungen durch:

- den Einsatz eines Code-Review-Prozesses zur Erhöhung der Sicherheit des zur Erbringung der Dienstleistungen verwendeten Codes und Prüfcodes und -systeme für Schwachstellen vor und während der Nutzung;
- Beibehaltung eines externen „bug bounty program“ (Fehler-Programm);
- Überprüfungen zur Validierung der Integrität verschlüsselter Daten und
- Verwendung präventiver und reaktiver Eindringungserkennung (Intrusion Detection).

Cloudflare setzt hochverfügbare Systeme in geografisch verteilten Rechenzentren ein.

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

- eine Autorisierungsrichtlinie für die Eingabe, das Lesen, Verändern und Löschen von Daten;
- Authentifizierung autorisierter Mitarbeiter unter Verwendung eindeutiger Authentifizierungsdaten (Passwörter) und harte Token;
- Benutzerkennungen, die nach einem Zeitraum der Inaktivität Benutzer automatisch abmelden;
- Schutz der Dateneingabe sowie des Lesens, der Veränderung und der Löschung gespeicherter Daten; und
- der Anforderung, Datenverarbeitungseinrichtungen (die Räume, die die Computerhardware und die dazugehörige Ausrüstung) verschlossen und sicher zu halten.

Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit und den Zugang zu Personenbezogenen Daten Im Falle eines physischen oder technischen Zwischenfalls rechtzeitig wiederherzustellen

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

- Notfallwiederherstellung und Geschäftsweiterführungspläne und -verfahren;
- geografisch verteilten Rechenzentren;

- redundanter Infrastruktur, einschließlich Stromversorgung und Internetverbindung;
- Backups, die an alternativen Standorten gespeichert werden und zur Wiederherstellung im Falle des Ausfalls der primären Systeme verwendet werden können; und
- Störfallmanagement-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 von Cloudflare's Security & Privacy Compliance Programm regelmäßig von externen Dritt-Prüfern getestet und bewertet. Dazu können jährliche ISO/IEC 27001-Audits gehören, AICPA SOC 2 Typ II, PCI DSS Level 1 und andere externe Audits. Ebenfalls werden Maßnahmen regelmäßig durch interne Revisionen sowie jährliche und gezielte Risikobewertungen geprüft.

Maßnahmen zur Nutzeridentifikation und -autorisierung

Cloudflare implementiert wirksame Maßnahmen für die Nutzerauthentifizierung und das Berechtigungsmanagement durch:

- Anwendung einer obligatorischen Zugangskontroll- und Authentifizierungsrichtlinie;
- Anwendung eines „zero-trust"-Modells für Identifizierung und Autorisierung,
- Authentifizierung autorisierter Mitarbeiter unter Verwendung einzigartiger Authentifizierungsdaten und einer starken Multifaktor-Authentifizierung, einschließlich der Verwendung physischer Hard-Token;
- Zuweisung und Verwaltung geeigneter Berechtigungen gemäß Funktion, Genehmigung und Ausnahmemanagement; und
- Anwendung des Grundsatzes des minimalen Zugangs.

Maßnahmen zum Schutz der Daten während der Übermittlung

Cloudflare setzt wirksame Maßnahmen ein, um die Personenbezogenen Daten bei der Übertragung davor zu schützen, von unbefugten Personen gelesen, kopiert, verändert oder gelöscht zu werden, einschließlich durch die folgenden Maßnahmen:

- Verwendung modernster Transport-Verschlüsselungsprotokolle zur Gewährleistung eines wirksamen Schutzes vor aktiven und passiven Angriffen mit öffentlich zugänglichen Ressourcen;
- Verwendung vertrauenswürdiger Zertifizierungsstellen und Infrastrukturen für öffentliche Schlüssel;
- Umsetzung von Schutzmaßnahmen gegen aktive und passive Angriffe auf Sende- und Empfangssysteme, die Transportverschlüsselung zur Verfügung stellen, wie angemessene Firewalls, gegenseitige TLS-Verschlüsselung, API-Authentifizierung und Verschlüsselung zum Schutz der Gateways und Pipelines, durch welche Daten reisen, sowie Prüfungen für Software-Schwachstellen und mögliche Backdoors;
- Einsatz wirksamer Verschlüsselungsalgorithmen und Parametrisierung, wie zum Beispiel mindestens 128-Bit-Schlüssellängen für symmetrische Verschlüsselung und mindestens 2048-Bit-RSA- oder 256-Bit-EC-Schlüssellängen für asymmetrische Algorithmen.
- Verwendung ordnungsgemäß implementierter und ordnungsgemäß instandgehaltener Software, abgedeckt im Rahmen eines Schwachstellenmanagement-Programms und durch Wirtschaftsprüfung auf Konformität geprüft;
- Durchsetzung sicherer Maßnahmen zur zuverlässigen Erstellung, Verwaltung, Speicherung und zum Schutz von Kodierungsschlüsseln; und

- Auditprotokoll, Überwachung und Tracking von Datenübertragungen.

Maßnahmen zum Schutz der Daten bei der Speicherung

Cloudflare setzt wirksame Maßnahmen zum Schutz Personenbezogener Daten durch die Steuerung und Begrenzung des Zugangs zu Systemen der Datenverarbeitung bei deren Speicherung ein sowie durch:

- Verwendung von Verschlüsselungsprotokollen, die dem neuesten Stand der Technik entsprechen und einen wirksamen Schutz gegen aktive und passive Angriffe mit Ressourcen bieten, von denen bekannt ist, dass sie den öffentlichen Behörden zur Verfügung stehen;
- Verwendung vertrauenswürdiger Zertifizierungsstellen und Infrastrukturen für öffentliche Schlüssel;
- Prüfung von Systemen, die Daten speichern, auf Software-Schwachstellen und mögliche Hintertüren;
- Einsatz wirksamer Verschlüsselungsalgorithmen und Parametrisierung, wie z.B. die Notwendigkeit, Personenbezogene Daten mit AES-XTS mit einer Schlüssellänge von 128-Bit oder länger zu verschlüsseln;
- Verwendung korrekt implementierter und ordnungsgemäß gewarteter Software, die von einem Programm zur Verwaltung von Sicherheitslücken abgedeckt ist und durch Audits auf Konformität geprüft wird;
- Durchsetzung sicherer Maßnahmen zur zuverlässigen Erstellung, Verwaltung, Speicherung und zum Schutz von Verschlüsselungsschlüsseln;
- Identifizierung und Genehmigung von Systemen und Nutzern mit Zugang zu Datenverarbeitungssystemen;
- Automatische Abmeldung von Nutzern nach einer gewissen Zeit der Inaktivität; und
- Audit-Protokollierung, Überwachung und Nachverfolgung des Zugriffs auf Datenverarbeitungs- und Speichersysteme.

Cloudflare implementiert Zugriffskontrollen für bestimmte Bereiche der Datenverarbeitungssysteme, um sicherzustellen, dass nur befugte Nutzer im Rahmen und in dem Umfang Zugriff auf die Personenbezogenen Daten haben, die durch ihre jeweilige Zugriffsberechtigung (Autorisierung) abgedeckt sind und dass Personenbezogene Daten nicht unbefugt gelesen, kopiert oder verändert werden können. Dies wird durch verschiedene Maßnahmen gewährleistet, darunter:

- Mitarbeiterrichtlinien und -schulungen in Bezug auf die Zugriffsrechte jedes Mitarbeiters auf die Personenbezogenen Daten;
- Anwendung eines „zero-trust“-Modells für Identifizierung und Autorisierung;
- Authentifizierung autorisierter Mitarbeiter unter Verwendung einzigartiger Authentifizierungsdaten und einer starken Multifaktor-Authentifizierung, einschließlich der Verwendung physischer Hard-Token;
- Überwachung der Handlungen jener Personen, die befugt sind, Personenbezogene Daten zu löschen, zu ergänzen oder zu modifizieren;
- Freigabe der Daten nur an autorisierte 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 Zugriffskontrollen, um zu verhindern, dass Unbefugte Zugang zu den Geräten zur Datenverarbeitung (namentlich Datenbank- und Anwendungsserver und zugehörige Hardware) erhalten, wenn die Personenbezogenen Daten verarbeitet oder genutzt werden, einschließlich durch:

- Schaffung sicherer Bereiche;

- Schutz und Beschränkung von Zugangswegen;
- Festlegung von Zugriffsberechtigungen für Mitarbeiter und Dritte, einschließlich der entsprechenden Dokumentation;
- jeder Zugriff auf Rechenzentren, in denen Personenbezogene Daten gehostet werden, wird protokolliert, überwacht und nachverfolgt; und
- Rechenzentren, in denen Personenbezogene Daten gehostet 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 Verfolgung des Zugangs zu Personenbezogenen Daten eingeführt, auch für Systemadministratoren und um sicherzustellen, dass die Daten gemäß den erhaltenen Anweisungen verarbeitet werden. Dies wird durch verschiedene Maßnahmen gewährleistet, darunter:

- Authentifizierung autorisierter Mitarbeiter unter Verwendung einzigartiger Authentifizierungsdaten und einer starken Multifaktor-Authentifizierung, einschließlich der Verwendung physischer Hard-Token;
- Anwendung eines „zero-trust"-Modells für Identifizierung und Autorisierung;
- Aufrechterhaltung aktueller Listen mit den Identifikationsdaten der Systemadministratoren;
- Festlegung von Maßnahmen zur Erkennung, Bewertung und Reaktion auf risikoreiche Anomalien;
- die Aufrechterhaltung sicherer, genauer und unveränderter Zugriffsprotokolle 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 Systeme Dritter. Konfigurationsstandards sollten den branchenüblichen Praktiken wie dem Center for Internet Security (CIS) Level 1 Maßstäben entsprechen. Automatisierte Mechanismen müssen eingesetzt werden, um die Basiskonfigurationen auf Produktionssystemen durchzusetzen und um unautorisierte Änderungen zu verhindern. Die 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. Standardmäßig werden Zugriffskonfigurationen auf „deny-all" gesetzt, und Standardpasswörter müssen geändert werden, um die Richtlinien von Cloudflare vor der Geräteinstallation im Cloudflare-Netzwerk oder unmittelbar nach der Software- oder Betriebssysteminstallation zu erfüllen. Systeme sind eingerichtet, um Systemzeituhren auf Basis der Internationalen Atomzeit oder der vereinbarten Universalzeit (UTC) zu synchronisieren und der Zugriff auf Zeitdaten ist auf autorisiertes Personal beschränkt.

Maßnahmen für interne IT und IT-Sicherheitsführung und -Management

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 Sicherheits und Datenschutz teilnehmen. Cloudflare beschränkt und schützt die Verarbeitung Personenbezogener Daten und hat dokumentiert und umgesetzt:

- ein formales Informations-Sicherheits-Management-System (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 Informationen Management System (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 von Kundendaten.

Cloudflare bewahrt Dokumentationen über technische und organisatorische Maßnahmen im Falle von Audits und zur Beweissicherung auf. Cloudflare trifft angemessene Maßnahmen, um zu gewährleisten, dass Personen, die bei ihr beschäftigt sind, und andere Personen am Arbeitsplatz die in diesem Anhang 2 genannten technischen und organisatorischen Maßnahmen kennen und einhalten.

Maßnahmen zur Zertifizierung/Prüfung von Prozessen und Produkten

Die Umsetzung der ISMS und der damit verbundenen Sicherheitsrisikomanagementprozesse von Cloudflare wurden extern nach dem Industriestandard ISO/IEC 27001 zertifiziert. Die Umsetzung des umfassenden PIMS von Cloudflare wurde extern nach ISO/IEC 27701 zertifiziert, sowohl als Auftragsverarbeiter und Verantwortlicher von Kundeninformationen.

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

Bei Übermittlungen an (Unter-) Auftragsverarbeiter sind auch die spezifischen technischen und organisatorischen Maßnahmen zu beschreiben, die der (Unter-) Auftragsverarbeiter zu ergreifen hat, um dem für die Verarbeitung Verantwortlichen Hilfe leisten zu können (und bei Übermittlungen von einem Auftragsverarbeiter an einen Unterauftragsverarbeiter an den Datenexporteur).

Maßnahme	**Beschreibung**
Zugang zum Selbstbedienungsservice um den Rechten der betroffenen Person, Löschung, Berichtigung usw. zu entsprechen	Möglichkeit sich über das Cloudflare Dashboard anzumelden um Personenbezogene Daten zu prüfen und zu bearbeiten.