Datenverarbeitungsnachtrag

Bitte lesen Sie diese Vereinbarung sorgfältig durch, da sie wichtige Informationen zu Ihren gesetzlichen Rechten und Rechtsbehelfen enthält.

Die englische Version der rechtlichen Vereinbarungen und Richtlinien gilt als die einzige aktuelle und gültige Version dieses Dokuments. Jede übersetzte Version wird nur zu Ihrem Komfort bereitgestellt, um das Lesen und Verstehen der englischen Version zu erleichtern. Etwaige übersetzte Versionen sind nicht rechtsverbindlich und können die englischen Versionen nicht ersetzen. Im Falle von Meinungsverschiedenheiten oder Konflikten haben die rechtlichen Vereinbarungen und Richtlinien in englischer Sprache Vorrang.

Data processing addendum

Letzte Überarbeitung: 2025-07-01, 12:52:40 Uhr

Dieser Datenverarbeitungsnachtrag (der "Addendum") wird von und zwischen Hostinger International Ltd. (einer zyprischen Gesellschaft mit beschränkter Haftung, eingetragene Adresse 61 Lordou Vironos str., 6023 Larnaca, Zypern) oder Hostinger UK Limited (britische Gesellschaft mit beschränkter Haftung, eingetragene Adresse Nwms Center, 31 Southampton Row, Office 3.11, 3rd Floor, London, England, WC1B 5 HJ) und gegebenenfalls durchgeführt Seine verbundenen Unternehmen ("Hostinger") und Sie ("Customer") und ist unserem angeschlossen und ergänzt es Nutzungsbedingungen und alle Vereinbarungen, die abgedeckte Dienste regeln (zusammen die "Nutzungsbedingungen").

1. DEFINITIONEN

1.1 Sofern in diesem Nachtrag nichts anderes definiert ist, haben alle großgeschriebenen Begriffe, die nicht in diesem Nachtrag definiert sind, die ihnen in den Nutzungsbedingungen zugewiesene Bedeutung.

"Affiliates" bezeichnet jede Entität, die von Hostinger kontrolliert wird, kontrolliert oder gemeinsam mit Hostinger kontrolliert wird.

“Covered Services” bedeutet gehostete Dienste, die unsere Verarbeitung personenbezogener Daten umfassen könnten, wie zum Beispiel: (1) Hosting-Dienste, (2) VPS-Dienste, (3) E-Mail-Dienste, (4) Domain-Dienste, (5) Website-Builder, (6) Hostinger Horizons, (7) Hostinger Reach.

“Customer Data” bezeichnet die personenbezogenen Daten aller betroffenen Personen, die von Hostinger im Rahmen des Hostinger-Netzwerks im Namen des Kunden gemäß oder im Zusammenhang mit den Nutzungsbedingungen verarbeitet werden.

“Datenschutzgesetze” bezeichnet alle Datenschutz- oder Datenschutzgesetze und -vorschriften, die für die Verarbeitung personenbezogener Daten im Rahmen des Abkommens gelten, einschließlich, aber nicht beschränkt auf, (i) die australischen Datenschutzgrundsätze und das australische Datenschutzgesetz (1988), (ii) Brasiliens Lei Geral de Proteção de Dados (LGPD), (iii) der California Consumer Privacy Act (CCPA), (iv) Kanadas Federal Personal Information Protection and Electronic Documents Act (PIPEDA), (v) die EU-DSGVO, (vi) alle nationalen Datenschutzgesetze, die im Rahmen oder gemäß der DSGVO (vii) der EU-Datenschutzrichtlinie (Richtlinie 2002/58/EG), (viii) Singapurs Personal Data Protection Act 2012 (PDPA), (ix) das Schweizer Bundesdatenschutzgesetz vom 19. Juni 1992 und seine Verordnung sowie (x) UK DSGVO oder Datenschutzgesetz 2018; jeweils in der jeweils geänderten, ersetzten oder ersetzten Fassung.

“EEA” bedeutet Europäischer Wirtschaftsraum.

“EU DSGVO” bezeichnet die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr sowie zur Aufhebung der Richtlinie 95/46/EG.

“EU-Standardvertragsklauseln” bezeichnet die Standarddatenschutzklauseln, die durch die Entscheidung 2021/914 der Europäischen Kommission vom 4. Juni 2021 genehmigt und durch Bezugnahme hierin aufgenommen wurden. Modul zwei (Controller to Processor) EU-Standardvertragsklauseln und Modul drei (Processor to Processor) EU-Standardvertragsklauseln stehen zum Download unter zur Verfügung EUR-Lex-Website&.

“Hostinger Network” bedeutet Hostingers Rechenzentrumseinrichtungen, Server, Netzwerkgeräte und Host-Softwaresysteme (z. B. virtuelle Firewalls), die in der Kontrolle von Hostinger liegen und zur Bereitstellung der abgedeckten Dienste verwendet werden.

“Security Incident” bedeutet einen Verstoß gegen die Sicherheit der Hostinger-Sicherheitsstandards, der zur versehentlichen oder rechtswidrigen Zerstörung, zum Verlust, zur Änderung, zur unbefugten Offenlegung oder zum unbefugten Zugriff auf Kundendaten auf von Hostinger verwalteten oder kontrollierten Systemen führt.

“Sicherheitsstandards” bezeichnet die diesem Nachtrag als Anhang 2 beigefügten Sicherheitsstandards.

"Empfindliche Daten" (a) Sozialversicherungsnummer, Passnummer, Führerscheinnummer oder ähnliche Kennung (oder irgendein Teil davon); (b) Kredit - oder Debitkartennummer (außer der gekürzten (letzten vier Ziffern) einer Kredit - oder Debitkarte),

Finanzinformationen, Bankkontonummern oder Passwörter; (c) Beschäftigungs, Finanz, genetische, biometrische oder Gesundheitsinformationen; (d) rassische, ethnische, politische oder religiöse Zugehörigkeit, Gewerkschaftsmitgliedschaft oder Informationen über das Sexualleben oder die sexuelle Orientierung; (e) Kontopasswörter, Mädchenname der Mutter oder Geburtsdatum; (f) Kriminalgeschichte; oder (g) alle anderen Informationen oder Informationskombinationen, die unter die Definition von "Sonderkategorien von Daten" gemäß DSGVO oder anderen geltenden Gesetzen oder Vorschriften in Bezug auf Privatsphäre und Datenschutz fallen.

"Sub-Processor" bezeichnet jeden Prozessor, der von Hostinger beauftragt wird, Daten im Namen des Kunden zu verarbeiten.

"UK DSGVO" bedeutet die EU-DSGVO in der geänderten und in britisches Recht übernommenen Fassung gemäß dem UK European Union (Withdrawal) Act 2018 und den geltenden Sekundärgesetzen, die im Rahmen dieses Gesetzes erlassen wurden.

"UK International Data Transfer Addendum" bezeichnet den internationalen Datenübertragungszusatz zu den EU-Standardvertragsklauseln, herausgegeben vom UK Information Commissioner, Version B1.0, in Kraft am 21. März 2022, hierin durch Bezugnahme aufgenommen. Der UK International Data Transfer Addendum steht zum Download unter zur Verfügung Website des britischen Informationskommissars

1.2 Die in diesem Addendum verwendeten Begriffe "Personal Data", "Data Subject", "Processing", "Controller" und "Processor" haben die in der EU-DSGVO angegebene Bedeutung, unabhängig davon, welche Datenschutzgesetze gelten.

2. UMFANG DER DATENVERARBEITUNG UND PARTEIENVERHÄLTNIS

2.1 Hostinger als Prozessor. Die Parteien erkennen Folgendes an und vereinbaren Folgendes: (i) dass Hostinger gemäß den Datenschutzgesetzen ein Verarbeiter von Kundendaten ist; (ii) dass der Kunde ein Controller oder gegebenenfalls Verarbeiter der Kundendaten gemäß den Datenschutzgesetzen ist; und (iii) dass jede Partei ihren Verpflichtungen aus den geltenden Datenschutzgesetzen in Bezug auf die Verarbeitung von Kundendaten nachkommt.

2.2 Einzelheiten zur Datenverarbeitung. Gegenstand der Verarbeitung von Kundendaten durch Hostinger ist die Durchführung der abgedeckten Dienste gemäß den Nutzungsbedingungen. Hostinger verarbeitet Kundendaten nur für die folgenden Zwecke: (i) Verarbeitung gemäß den Nutzungsbedingungen; (ii) Verarbeitung, die von Endbenutzern bei der Nutzung der abgedeckten Dienste initiiert wird; (iii) Verarbeitung zur Einhaltung anderer dokumentierter, angemessener Anweisungen der Kunden (z. B. per E-Mail), sofern diese Anweisungen mit den Nutzungsbedingungen im Einklang stehen. Hostinger darf: (a) Kundendaten nicht verarbeiten, speichern, nutzen, verkaufen oder offenlegen, es sei denn, dies ist für die Bereitstellung abgedeckter Dienste gemäß den Nutzungsbedingungen oder gemäß den gesetzlichen Bestimmungen erforderlich; (b) solche Kundendaten an Dritte verkaufen; (c) diese Kundendaten außerhalb der direkten Geschäftsbeziehung zwischen Hostinger und Kunde aufbewahren, verwenden oder offenlegen, sofern gesetzlich nichts anderes vorgeschrieben ist.

Um Zweifel auszuschließen, muss die Verarbeitung von Kundendaten allen Datenschutzgesetzen entsprechen. Der Kunde trägt die alleinige Verantwortung für die Richtigkeit, Qualität und Rechtmäßigkeit der Kundendaten sowie für die Mittel, mit denen der Kunde Kundendaten erfasst hat. Wenn der Kunde ein Controller der Kundendaten ist, erkennt der Kunde Folgendes an und stimmt ihm zu: (i) Der Kunde muss wirtschaftlich angemessene Anstrengungen unternehmen, um die Datenerfassung, -weitergabe und -nutzung, die bei allen abgedeckten Diensten stattfindet, klar offenzulegen und deren Zustimmung einzuholen; und (ii) Der Kunde muss klarstellen, dass als Folge Ihrer Nutzung der abgedeckten Dienste Die Daten des Endnutzers dürfen außerhalb ihres Herkunftslandes verarbeitet werden. Wenn der Kunde ein Verarbeiter der Kundendaten ist, garantiert der Kunde, dass die Anweisungen und Maßnahmen des Kunden in Bezug auf Kundendaten, einschließlich der Ernennung von Hostinger zu einem anderen Verarbeiter, vom jeweiligen Verantwortlichen genehmigt wurden. Hostinger ist nicht verpflichtet, den Anweisungen des Kunden Folge zu leisten oder diese zu befolgen, wenn diese Anweisungen gegen Datenschutzgesetze verstoßen würden. Die Dauer der Verarbeitung, die Art und der Zweck der Verarbeitung, die Arten personenbezogener Daten und Kategorien der im Rahmen dieses Nachtrags verarbeiteten betroffenen Personen sind in Anhang 1 (‘Details der Verarbeitung’) dieses Nachtrags näher erläutert.

3. VERTRAULICHKEIT DER KUNDENDATEN

Hostinger wird Kundendaten nicht an eine Regierung oder andere Dritte weitergeben, es sei denn, dies ist zur Einhaltung des Gesetzes oder einer gültigen und verbindlichen Anordnung einer Strafverfolgungsbehörde (z. B. einer Vorladung oder einem Gerichtsbeschluss) erforderlich. Für den Fall, dass Hostinger eine gültige zivilrechtliche Vorladung erhält, und im zulässigen Umfang wird sich Hostinger bemühen, den Kunden über die Forderung angemessen per E-Mail oder Post zu informieren, damit der Kunde eine Schutzanordnung oder einen anderen geeigneten Rechtsbehelf einholen kann (sofern nicht anders erforderlich Vorladung, Gerichtsbeschluss oder ein anderes gültiges Rechtsdokument).

4. SHARED-RESPONSIBILITY-MODELL DER SICHERHEIT

4.1 Hostinger hat die technischen und organisatorischen Maßnahmen für das Hostinger-Netzwerk umgesetzt und wird diese aufrechterhalten, wie in diesem Abschnitt beschrieben und in Anhang 2 dieses Addendums, Sicherheitsstandards, näher beschrieben. Hostinger hat insbesondere die folgenden technischen und organisatorischen Maßnahmen umgesetzt und wird diese aufrechterhalten, die sich mit (i) der Sicherheit des Hostinger-Netzwerks befassen; (ii) physische Sicherheit der Einrichtungen; (iii) Kontrollen des Zugangs von Mitarbeitern und Auftragnehmern zu (i) und/oder (ii); und (iv) Prozesse zum Testen, Beurteilung und Bewertung der Wirksamkeit der von Hostinger durchgeführten technischen und organisatorischen Maßnahmen. Für den Fall, dass wir einer unserer hier dargelegten Verpflichtungen nicht nachkommen können, werden wir dies so schnell wie praktisch möglich schriftlich mitteilen (über unsere Website oder E-Mail).

4.2 Hostinger stellt eine Reihe von Sicherheitsfunktionen und Funktionalitäten zur Verfügung, die der Kunde in Bezug auf die abgedeckten Dienste nutzen kann. Der Kunde ist verantwortlich für (a) die ordnungsgemäße Konfiguration der abgedeckten Dienste, (b) die Verwendung der im Zusammenhang mit den abgedeckten Diensten verfügbaren Kontrollen (einschließlich der Sicherheitskontrollen), um die fortlaufende Vertraulichkeit, Integrität,

Verfügbarkeit und Widerstandsfähigkeit der Verarbeitungssysteme und -dienste sicherzustellen, (c) Ergreifen der Schritte, die Hostinger für angemessen hält, um angemessene Sicherheit, Schutz und Löschung von Kundendaten aufrechtzuerhalten Dazu gehören der Einsatz von Verschlüsselungstechnologie zum Schutz von Kundendaten vor unbefugtem Zugriff und Maßnahmen zur Kontrolle der Zugriffsrechte auf Kundendaten.

5. RECHTE DER BETROFFENEN PERSON

Unter Berücksichtigung der Art der abgedeckten Dienste bietet Hostinger dem Kunden bestimmte Kontrollen an, die der Kunde möglicherweise zum Abrufen, Berichtigen, Löschen oder Einschränken der Nutzung und Weitergabe von Kundendaten verwendet, wie in den abgedeckten Diensten beschrieben. Der Kunde kann diese Kontrollen als technische und organisatorische Maßnahmen nutzen, um ihn im Zusammenhang mit seinen Verpflichtungen aus den Datenschutzgesetzen zu unterstützen, einschließlich seiner Verpflichtungen im Zusammenhang mit der Beantwortung von Anfragen von betroffenen Personen. Soweit wirtschaftlich sinnvoll und soweit rechtmäßig erforderlich oder zulässig, muss Hostinger den Kunden unverzüglich benachrichtigen, wenn Hostinger direkt eine Anfrage von einer betroffenen Person erhält, diese Rechte gemäß den geltenden Datenschutzgesetzen auszuüben (“Data Subject Request”). Wenn darüber hinaus die Nutzung der abgedeckten Dienste durch den Kunden seine Fähigkeit einschränkt, eine Anfrage einer betroffenen Person zu bearbeiten, kann Hostinger, sofern gesetzlich zulässig und angemessen und auf ausdrücklichen Wunsch des Kunden, dies tun Bereitstellung wirtschaftlich angemessener Unterstützung bei der Bearbeitung der Anfrage auf Kosten des Kunden (falls vorhanden).

6. UNTERVERARBEITUNG

6.1 Autorisierte Unterauftragsverarbeiter. Der Kunde stimmt zu, dass Hostinger Unterauftragsverarbeiter nutzen kann, um seinen vertraglichen Verpflichtungen gemäß seinen Nutzungsbedingungen und diesem Nachtrag nachzukommen oder bestimmte Dienstleistungen in seinem Namen bereitzustellen, beispielsweise die Bereitstellung von Supportdiensten. Der Kunde stimmt hiermit der Verwendung von Unterverarbeitern durch Hostinger zu, wie in diesem Abschnitt beschrieben.

6.2 Pflichten des Unterauftragsverarbeiters. Wenn Hostinger einen autorisierten Unterverarbeiter verwendet, wie in Abschnitt 6.1 beschrieben:

(i) Hostinger beschränkt den Zugriff des Unterauftragsverarbeiters auf Kundendaten nur auf das, was zur Aufrechterhaltung der abgedeckten Dienste oder zur Bereitstellung der abgedeckten Dienste für den Kunden und alle Endbenutzer gemäß den Nutzungsbedingungen erforderlich ist. Hostinger wird dem Unterverarbeiter den Zugriff auf Kundendaten für andere Zwecke verbieten;

(ii) Hostinger wird eine schriftliche Vereinbarung mit dem Unterverarbeiter abschließen und, sofern der Unterverarbeiter dieselben Datenverarbeitungsdienste erbringt, die Hostinger im Rahmen dieses Nachtrags erbringt, dem Unterverarbeiter auferlegen im Wesentlichen ähnliche vertragliche Verpflichtungen, die Hostinger im Rahmen dieses Nachtrags hat; Und

(iii) Hostinger bleibt für die Einhaltung der Verpflichtungen dieses Nachtrags und für alle Handlungen oder Unterlassungen des Unterauftragsverarbeiters verantwortlich, die dazu

führen, dass Hostinger gegen eine der Verpflichtungen von Hostinger gemäß diesem Nachtrag verstößt.

6.3 Neue Unterauftragsverarbeiter. Von Zeit zu Zeit kann Hostinger gemäß und vorbehaltlich der Bedingungen dieses Nachtrags neue Unterauftragsverarbeiter beauftragen. Neue Unterprozessoren werden dem Anhang 3 hinzugefügt. Wenn der Kunde einem neuen Unterauftragsverarbeiter nicht zustimmt, kann der Kunde alle abgedeckten Dienste ohne Vertragsstrafe kündigen, indem er innerhalb von 10 Tagen oder nach Erhalt der Mitteilung von Hostinger eine schriftliche Kündigung mit einer Erläuterung der Gründe für Ihre Nichtgenehmigung vorlegt. Wenn die abgedeckten Dienste Teil eines Pakets oder eines gebündelten Kaufs sind, gilt jede Kündigung für den gesamten Betrag.

7. SICHERHEITSVORFALL

7.1 Sicherheitsvorfall. Wenn Hostinger von einem Sicherheitsvorfall erfährt, wird Hostinger unverzüglich Folgendes tun: (a) den Kunden über den Sicherheitsvorfall informieren; und (b) angemessene Maßnahmen ergreifen, um die Auswirkungen abzumildern und etwaige durch den Sicherheitsvorfall verursachte Schäden zu minimieren.

7.2 Hostinger-Unterstützung. Um den Kunden in Bezug auf Benachrichtigungen über Verstöße gegen personenbezogene Daten zu unterstützen, die der Kunde gemäß den Datenschutzgesetzen machen muss, wird Hostinger in die Benachrichtigung solche Informationen über den Sicherheitsvorfall aufnehmen, die Hostinger dem Kunden unter Berücksichtigung der Art des Sicherheitsvorfalls vernünftigerweise offenlegen kann Abgedeckte Dienste, die Hostinger zur Verfügung stehenden Informationen und etwaige Einschränkungen bei der Offenlegung der Informationen, wie z. B. Vertraulichkeit.

7.3 Gescheiterte Sicherheitsvorfälle. Der Kunde stimmt zu, dass ein fehlgeschlagener Sicherheitsvorfall nicht den Bedingungen dieses Nachtrags unterliegt. Ein fehlgeschlagener Sicherheitsvorfall führt zu keinem unbefugten Zugriff auf Kundendaten oder auf das Netzwerk, die Ausrüstung oder die Einrichtungen von Hostinger, die Kundendaten speichern, und kann unter anderem Pings und andere Broadcast-Angriffe auf Firewalls oder Edge-Server sowie Portscans umfassen, erfolglose Anmeldeversuche, Denial-of-Service-Angriffe, Paket-Sniffing (oder anderer unbefugter Zugriff auf Verkehrsdaten, der nicht zu einem Zugriff jenseits von Headern führt) oder ähnliche Vorfälle.

7.4 Benachrichtigung. Benachrichtigungen über Sicherheitsvorfälle, falls vorhanden, werden auf beliebige Weise, die Hostinger auswählt, an einen oder mehrere Administratoren des Kunden übermittelt, auch per E-Mail. Es liegt in der alleinigen Verantwortung des Kunden, sicherzustellen, dass die Administratoren des Kunden jederzeit genaue Kontaktinformationen auf der Hostinger-Verwaltungskonsole und eine sichere Übertragung speichern.

7.5 Kein Eingeständnis eines Verschuldens durch Hostinger: Hostingers Verpflichtung, einen Sicherheitsvorfall gemäß diesem Abschnitt zu melden oder darauf zu reagieren, ist und wird nicht als Eingeständnis eines Verschuldens oder einer Haftung von Hostinger in Bezug auf den Sicherheitsvorfall durch Hostinger ausgelegt.

8. KUNDENRECHTE

8.1 Unabhängige Bestimmung. Der Kunde ist dafür verantwortlich, die von Hostinger zur Verfügung gestellten Informationen in Bezug auf die Datensicherheit und ihre Sicherheitsstandards zu überprüfen und eine unabhängige Feststellung darüber zu treffen, ob die abgedeckten Dienste den Anforderungen und rechtlichen Verpflichtungen des Kunden sowie den Verpflichtungen des Kunden gemäß diesem Nachtrag entsprechen. Die zur Verfügung gestellten Informationen sollen den Kunden bei der Einhaltung der Verpflichtungen des Kunden gemäß den geltenden Datenschutzgesetzen unterstützen. Der Kunde erklärt sich damit einverstanden, dass die abgedeckten Dienste und die von Hostinger implementierten und gepflegten Sicherheitsstandards ein dem Risiko für personenbezogene Daten angemessenes Sicherheitsniveau bieten (unter Berücksichtigung des Stands der Technik, der Kosten für die Umsetzung sowie der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung personenbezogener Daten sowie der Risiken für Einzelpersonen).

8.2 Rechte der Kundenprüfung. Der Kunde hat das Recht, die Einhaltung dieses Addendums durch Hostinger in Bezug auf die abgedeckten Dienste zu bestätigen, indem er in angemessenen Abständen eine spezifische schriftliche Anfrage an die in den Nutzungsbedingungen angegebene Adresse stellt. Wenn Hostinger sich weigert, den vom Kunden angeforderten Anweisungen bezüglich einer ordnungsgemäß angeforderten und umfangreichen Prüfung oder Inspektion Folge zu leisten, ist der Kunde berechtigt, diesen Nachtrag und die Nutzungsbedingungen zu kündigen.

9. ÜBERTRAGUNGEN VON KUNDENDATEN

9.1 Anwendung von EU-Standardvertragsklauseln. Modul Zwei (Controller to Processor) EU-Standardvertragsklauseln oder Modul Drei (Processor to Processor) EU-Standardvertragsklauseln gelten für Kundendaten, die außerhalb des EWR entweder direkt oder per Weiterübertragung in ein Land übertragen werden, das von der Europäischen Kommission nicht anerkannt wird als ein angemessenes Schutzniveau für Kundendaten. Diese EU-Standardvertragsklauseln gelten nicht für Kundendaten, die nicht direkt oder per Weiterleitung außerhalb des EWR übertragen werden. Ungeachtet des Vorstehenden finden diese EU-Standardvertragsklauseln keine Anwendung, wenn die Daten gemäß einem anerkannten Compliance-Standard für die rechtmäßige Übermittlung personenbezogener Daten außerhalb des EWR übertragen werden, beispielsweise wenn dies für die Erbringung abgedeckter Dienste gemäß den Bedingungen erforderlich ist Service oder mit Ihrer Zustimmung.

1. Für jedes Modul, sofern zutreffend:
    1. In Klausel 7 der EU-Standardvertragsklauseln gilt die optionale Andockklausel nicht;
    2. In Klausel 9 der EU-Standardvertragsklauseln gilt Option 2 und die Frist für die vorherige schriftliche Mitteilung von Änderungen an Unterverwaltern ist in Abschnitt 6.3 (Neue Unterverarbeiter) dieses Nachtrags festgelegt;
    3. In Klausel 11 der EU-Standardvertragsklauseln ist die optionale Sprache Englisch;
    4. In Klausel 17 (Option 1) unterliegen die EU-Standardvertragsklauseln zyprischem Recht;

5. In Klausel 18 (b) der EU-Standardvertragsklauseln werden Streitigkeiten vor den Gerichten Zyperns beigelegt;
6. In Anhang I Teil A der EU-Standardvertragsklauseln:
    - Liste der Parteien

      Datenexporteur (e): Der Datenexporteur ist das Unternehmen, das im Nachtrag als “Customer” identifiziert wurde
      Unterschrift und Datum: Ab dem Datum der elektronischen Annahme der Nutzungsbedingungen des Datenexporteurs durch den Datenexporteur wird davon ausgegangen, dass der Datenexporteur diese EU-Standardvertragsklauseln unterzeichnet hat.
      Rolle: Controller (unter Modul Zwei) oder Prozessor (unter Modul Drei)

      Datenimporteur (e): Hostinger International Ltd.
      Kontaktdaten: gdpr@hostinger.com
      Unterschrift und Datum: Ab dem Datum der elektronischen Annahme der Nutzungsbedingungen des Datenimporteurs durch den Datenexporteur wird davon ausgegangen, dass der Datenimporteur diese EU-Standardvertragsklauseln unterzeichnet hat.
      Rolle: Prozessor
7. In Anhang 1 Teil B der EU-Standardvertragsklauseln:
    - Beschreibung der Übertragung

      Kategorien von betroffenen Personen, deren personenbezogene Daten übertragen werden, sind in Anhang 1 des Addendums beschrieben.
      Kategorien der übertragenen personenbezogenen Daten sind in Anhang 1 des Addendums beschrieben. Die übertragenen sensiblen Daten sind in Anhang 1 dieses Nachtrags beschrieben.
      Die Häufigkeit der Übertragung ist eine kontinuierliche Grundlage für die Dauer der Nutzungsbedingungen.
      Die Art der Verarbeitung ist in Abschnitt 2.2 und Anhang 1 des Addendums beschrieben.
      Zweck (e) der Datenübertragung und der weiteren Verarbeitung sind in Abschnitt 2.2 und Anlage 1 dieses Addendums beschrieben.
      Der Zeitraum, für den die personenbezogenen Daten gespeichert werden, ist in Anhang 1 dieses Nachtrags beschrieben.
      Für Übertragungen an (Unter-)Verarbeiter sind Gegenstand, Art und Dauer der Verarbeitung in Anlage 3 zu den Standardvertragsklauseln festgelegt.
8. In Anhang 1 Teil C der EU-Standardvertragsklauseln:
    - Zuständige Aufsichtsbehörde
      Das Büro des Beauftragten für den Schutz personenbezogener

Daten (Zypern) ist die zuständige Aufsichtsbehörde.

9. In Anhang 2 der EU-Standardvertragsklauseln:

   Die vom Datenimporteur umgesetzten technischen und organisatorischen Sicherheitsmaßnahmen sind in Anhang 2 des Addendums aufgeführt.

10. In Anhang 3 der EU-Standardvertragsklauseln:

    Die Liste der Unterauftragsverarbeiter finden Sie in Anhang 3 dieses Nachtrags.

9.3 Anwendung des UK International Data Transfer Addendum. Der UK International Data Transfer Addendum gilt für Kundendaten, die über abgedeckte Dienste aus dem Vereinigten Königreich entweder direkt oder per Weiterübertragung an ein Land übermittelt werden, das von der zuständigen Regulierungsbehörde des Vereinigten Königreichs oder einer Regierungsbehörde nicht als Land anerkannt wird, das ein angemessenes Schutzniveau bietet Kundendaten. Der UK International Data Transfer Addendum gilt nicht für Kundendaten, die nicht direkt oder per Weiterübertragung außerhalb des Vereinigten Königreichs übertragen werden. Ungeachtet des Vorstehenden findet das UK International Data Transfer Addendum keine Anwendung, wenn die Daten gemäß einem anerkannten Compliance-Standard für die rechtmäßige Übermittlung von Kundendaten außerhalb des Vereinigten Königreichs übertragen werden, beispielsweise wenn dies für die Erbringung der abgedeckten Dienste gemäß erforderlich ist die Nutzungsbedingungen oder mit Ihrer Zustimmung.

1. Für Datenübermittlungen aus dem Vereinigten Königreich, die dem UK International Data Transfer Addendum unterliegen, gilt das UK International Data Transfer Addendum als eingegeben (und durch diese Referenz in dieses Addendum aufgenommen) und wie folgt vervollständigt:
    1. In Tabelle 1 des UK International Data Transfer Addendum finden Sie die Einzelheiten und wichtigsten Kontaktinformationen der Parteien in Abschnitt 9.2 (i) (f) dieses Addendums.
    2. In Tabelle 2 des UK International Data Transfer Addendum finden sich Informationen über die Version der EU-Standardvertragsklauseln, Module und ausgewählten Klauseln, denen dieser UK International Data Transfer Addendum beigefügt ist, in Abschnitt 9.2 (EU-Standardvertragsklauseln) dieses Addendums.
    3. In Tabelle 3 des UK International Data Transfer Addendum:
        1. Die Liste der Parteien befindet sich in Abschnitt 9.2 (i) (f) dieses Addendums.
        2. Die Beschreibung der Übertragung ist in Abschnitt 1 (Art und Zweck der Verarbeitung) von Anlage 1 (Einzelheiten der Verarbeitung) dieses Nachtrags enthalten.
        3. Anhang 2 befindet sich in Anhang 2 (Sicherheitsstandards) dieses Nachtrags
        4. Die Liste der Unterauftragsverarbeiter ist in Anhang 3 dieses Addendums enthalten.

4. In Tabelle 4 des UK International Data Transfer Addendum können sowohl der Importeur als auch der Exporteur den UK International Data Transfer Addendum gemäß den Bedingungen des UK International Data Transfer Addendum beenden.

10. BEENDIGUNG DES NACHTRAGS

Dieser Nachtrag bleibt bis zur Beendigung unserer Verarbeitung gemäß den Nutzungsbedingungen ("Kündigungsdatum") in Kraft.

11. RÜCKGABE ODER LÖSCHUNG VON KUNDENDATEN

Wie in den abgedeckten Diensten beschrieben, können dem Kunden Steuerelemente bereitgestellt werden, die zum Abrufen oder Löschen von Kundendaten verwendet werden können. Die Löschung der Kundendaten erfolgt dreißig (30) Tage nach dem Kündigungsdatum, vorbehaltlich der Bedingungen der jeweiligen abgedeckten Dienste. Der Kunde erkennt an, dass es in der Verantwortung des Kunden liegt, vor dem Kündigungsdatum alle Kundendaten zu exportieren, die Sie nach dem Kündigungsdatum speichern möchten.

12. HAFTUNGSBESCHRÄNKUNGEN

Die Haftung jeder Partei im Rahmen dieses Nachtrags unterliegt den in den Nutzungsbedingungen festgelegten Haftungsausschlüssen und -beschränkungen. Der Kunde stimmt zu, dass alle regulatorischen Strafen, die Hostinger in Bezug auf die Kundendaten auferlegt werden und die sich aus oder im Zusammenhang mit der Nichteinhaltung der Verpflichtungen des Kunden aus diesem Nachtrag und allen geltenden Datenschutzgesetzen ergeben, auf die Haftung von Hostinger angerechnet und verringert werden gemäß den Nutzungsbedingungen, als ob es eine Haftung gegenüber dem Kunden gemäß den Nutzungsbedingungen wäre.

13. GESAMTE NUTZUNGSBEDINGUNGEN; KONFLIKT

Dieser Nachtrag ersetzt und ersetzt alle vorherigen oder gleichzeitigen Zusicherungen, Vereinbarungen, Vereinbarungen oder Mitteilungen zwischen Kunde und Hostinger, ob schriftlich oder mündlich, in Bezug auf den Gegenstand dieses Nachtrags, einschließlich aller zwischen Hostinger und Kunde in Bezug auf die Datenverarbeitung eingegangenen Nachträge Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Soweit ein Konflikt oder eine Inkonsistenz zwischen den EU-Standardvertragsklauseln oder dem UK International Data Transfer Addendum und allen anderen Bedingungen in diesem Addendum oder den Nutzungsbedingungen besteht, gelten die Bestimmungen der EU-Standardvertragsklauseln oder des UK International Data Transfer Addendum. soweit zutreffend, hat Vorrang. Sofern durch diesen Nachtrag nichts anderes geändert wird, bleiben die Nutzungsbedingungen in vollem Umfang in Kraft und wirksam. Wenn ein Konflikt zwischen den Nutzungsbedingungen und diesem Nachtrag besteht, gelten die Bedingungen dieses Nachtrags.

ANHANG 1

EINZELHEITEN DER VERARBEITUNG

1. Art und Zweck der Verarbeitung. Hostinger verarbeitet Kundendaten nach Bedarf zur Erbringung der abgedeckten Dienste gemäß den Nutzungsbedingungen und gemäß den weiteren Anweisungen des Kunden während der gesamten Nutzung der abgedeckten Dienste.

2. Dauer der Verarbeitung. Vorbehaltlich der Abschnitte 10 und 11 dieses Nachtrags verarbeitet Hostinger Kundendaten während des Inkrafttretens der Nutzungsbedingungen. Ungeachtet des Vorstehenden kann Hostinger Kundendaten oder Teile davon aufbewahren, sofern dies durch geltende Gesetze oder Vorschriften, einschließlich der geltenden Datenschutzgesetze, erforderlich ist, vorausgesetzt, dass diese Kundendaten gemäß den Bedingungen dieses Nachtrags und den geltenden Datenschutzgesetzen geschützt bleiben.

3. Kategorien von betroffenen Personen. Der Kunde kann im Rahmen seiner Nutzung der abgedeckten Dienste personenbezogene Daten hochladen, deren Umfang vom Kunden nach eigenem Ermessen festgelegt und kontrolliert wird und zu denen unter anderem personenbezogene Daten in Bezug auf die folgenden Kategorien von Daten gehören können Themen:

- Interessenten, Kunden, Geschäftspartner und Kundenverkäufer (bei denen es sich um natürliche Personen handelt)
- Mitarbeiter oder Ansprechpartner der Interessenten, Kunden, Geschäftspartner und Lieferanten des Kunden
- Mitarbeiter, Vertreter, Berater, Freiberufler des Kunden (bei denen es sich um natürliche Personen handelt)
- Vom Kunden autorisierte Benutzer des Kunden zur Nutzung der abgedeckten Dienste

4. Kategorien personenbezogener Daten. Der Kunde kann im Rahmen seiner Nutzung der abgedeckten Dienste personenbezogene Daten hochladen, deren Art und Umfang vom Kunden nach eigenem Ermessen festgelegt und kontrolliert wird und die die folgenden Kategorien personenbezogener Daten umfassen können, aber nicht darauf beschränkt sind der betroffenen Personen:

- Name
- Adresse
- Telefonnummer
- Geburtsdatum
- E-mail-adresse
- Sonstige gesammelte Daten, die direkt oder indirekt betroffene Personen identifizieren könnten.

5. Sensible Daten oder spezielle Datenkategorien. Der Kunde kann sensible Daten im Rahmen seiner Nutzung der abgedeckten Dienste hochladen, deren Art und Umfang vom Kunden nach eigenem Ermessen festgelegt und kontrolliert wird. Der Kunde ist dafür verantwortlich, Einschränkungen oder Schutzmaßnahmen anzuwenden, die die Art der Daten und die damit verbundenen Risiken vor der Übermittlung oder Verarbeitung sensibler Daten über die abgedeckten Dienste vollständig berücksichtigen.

ANHANG 2

SICHERHEITSSTANDARDS

ICH. Technische und organisatorische Maßnahmen

Wir verpflichten uns, die Informationen unserer Kunden zu schützen. Unter Berücksichtigung der Best Practices, der Umsetzungskosten sowie der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen ergreifen wir die folgenden technischen und organisatorischen Maßnahmen. Bei der Auswahl der Maßnahmen werden die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme berücksichtigt.

II. Datenschutzprogramm

Unser Datenschutzprogramm wurde eingerichtet, um während seines gesamten Lebenszyklus eine globale Datenverwaltungsstruktur aufrechtzuerhalten und Informationen zu sichern. Wir testen, bewerten und bewerten regelmäßig die Wirksamkeit seines Datenschutzprogramms und seiner Sicherheitsstandards.

1. Vertraulichkeit. "Vertraulichkeit bedeutet, dass personenbezogene Daten vor unbefugter Offenlegung geschützt sind."

Wir nutzen eine Vielzahl physischer und logischer Maßnahmen, um die Vertraulichkeit der personenbezogenen Daten unserer Kunden zu schützen. Zu diesen Maßnahmen gehören:

Physische Sicherheit

- Physische Zugangskontrollsysteme vorhanden (Badge-Zugangskontrolle, Überwachung von Sicherheitsereignissen usw)
- Überwachungssysteme einschließlich Alarme und gegebenenfalls CCTV-Überwachung
- Vernichtung von Daten zu physischen Dokumenten (Zerkleinerung)

Zugangskontrolle & Verhinderung unbefugten Zugriffs

- Angewandte Benutzerzugriffsbeschränkungen und bereitgestellte/überprüfte rollenbasierte Zugriffsberechtigungen basierend auf dem Prinzip der Aufgabentrennung
- Starke Authentifizierungs - und Autorisierungsmethoden
- Zentralisierte Passwortverwaltung und starke/komplexe Passwortrichtlinien (Mindestlänge, Komplexität der Zeichen, Ablauf von Passwörtern etc)
- Kontrollierter Zugriff auf E-Mails und das Internet
- Antivirenmanagement

Verschlüsselung

- Verschlüsselung externer und interner Kommunikation über starke kryptografische Protokolle
- Verschlüsselung personenbezogener Daten und sensibler Daten im Ruhezustand (Datenbanken, gemeinsam genutzte Verzeichnisse usw)

- Vollständige Festplattenverschlüsselung für Firmen-PCs und Laptops
- Fernverbindungen zu den Unternehmensnetzwerken werden per VPN verschlüsselt

Datenminimierung

- PII/SPI-Minimierung in Anwendungs-, Debugging- und Sicherheitsprotokollen
- Pseudonymisierung personenbezogener Daten, um eine direkte Identifizierung einer Person zu verhindern
- Trennung der gespeicherten Daten nach Funktion (Test, Staging, Live)
- Logische Trennung der Daten nach rollenbasierten Zugriffsrechten
- Definierte Datenaufbewahrungsfristen für personenbezogene Daten

Sicherheitsprüfung

- Penetrationstests für kritische Unternehmensnetzwerke und Plattformen, die personenbezogene Daten hosten
- Regelmäßige Netzwerk- und Schwachstellenscans

2. Integrität. “Integrität bezieht sich auf die Gewährleistung der Korrektheit (Intaktheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität im Zusammenhang mit dem Begriff "Daten" verwendet wird, drückt er aus, dass die Daten vollständig und unverändert sind.”

Zusätzlich zu den Zugriffskontrollen sind geeignete Änderungs- und Protokollverwaltungskontrollen vorhanden, um die Integrität personenbezogener Daten aufrechterhalten zu können, wie zum Beispiel:

Änderungs- und Freigabeverwaltung

- Änderungs - und Freigabeprozess einschließlich (Wirkungsanalyse, Genehmigungen, Tests, Sicherheitsüberprüfungen, Inszenierung, Überwachung usw)
- Rollen- und funktionsbasierte (Segregation of Duties) Zugriffsbereitstellung auf Produktionsumgebungen

Protokollierung und Überwachung

- Protokollierung von Zugriffen und Änderungen der Daten
- Zentralisierte Audit- und Sicherheitsprotokolle
- Überwachung der Vollständigkeit und Richtigkeit der Datenübermittlung (End-to-End-Check)

3. Verfügbarkeit. “Die Verfügbarkeit von Diensten und IT-Systemen, IT-Anwendungen und IT-Netzwerkfunktionen bzw. von Informationen ist gewährleistet, wenn die Nutzer diese jederzeit wie vorgesehen nutzen können.”

Wir implementieren geeignete Kontinuitäts- und Sicherheitsmaßnahmen, um die Verfügbarkeit seiner Dienste und der in diesen Diensten gespeicherten Daten aufrechtzuerhalten:

- Regelmäßige Failover-Benachrichtigungen gelten für kritische Dienste

- Umfangreiche Leistungs-/Verfügbarkeitsüberwachung und Berichterstattung für kritische Systeme
- Reaktionsprogramm
- Kritische Daten entweder repliziert oder gesichert (Cloud Backups/Hard Disks/Datenbankreplikation usw)
- Geplante Software, Infrastruktur - und Sicherheitswartung vorhanden (Software-Updates, Sicherheitspatches etc)
- Verwendung unterbrechungsfreier Stromversorgungen, ausfallende redundante Hardware und Netzwerksysteme
- Alarm, Sicherheitssysteme vorhanden
- Physische Schutzmaßnahmen für kritische Stellen (Überspannungsschutz, Doppelböden, Kühlsysteme, Brand- und/oder Rauchmelder, Brandbekämpfungssysteme usw.)
- DDOS-Schutz zur Aufrechterhaltung der Verfügbarkeit
- Belastungs- und Stresstests

4. Anweisungen zur Datenverarbeitung. "Anweisungen zur Datenverarbeitung beziehen sich darauf, sicherzustellen, dass personenbezogene Daten nur in Übereinstimmung mit den Anweisungen des Datenverantwortlichen und den damit verbundenen Maßnahmen des Unternehmens verarbeitet werden"

Wir haben interne Datenschutzrichtlinien und -vereinbarungen festgelegt und führen regelmäßig Datenschutzschulungen für Mitarbeiter durch, um sicherzustellen, dass personenbezogene Daten gemäß den Präferenzen und Anweisungen des Kunden' verarbeitet werden.

- Datenschutz- und Vertraulichkeitsbedingungen in Arbeitnehmerverträgen
- Regelmäßige Datenschutz- und Sicherheitsschulungen für Mitarbeiter
- Geeignete vertragliche Bestimmungen zu den Vereinbarungen mit Subunternehmern zur Wahrung der Weisungskontrollrechte
- Regelmäßige Datenschutzprüfungen für externe Dienstleister
- Bereitstellung der vollständigen Kontrolle über die Datenverarbeitungspräferenzen für Kunden

ANHANG 3

UNTERPROZESSOREN

- AMAZON WEB SERVICES EMEA SARL
- Google Cloud EMEA Limited
- Cloudflare, Inc.
- MailChannels Corporation
- Proofpoint, Inc.
- Anthropic Ireland, Limited
- Spektrentechnologie, UAB

HOSTING
DOMÄNE
WERKZEUGE
INFORMATION
UNTERNEHMEN
UNTERSTÜTZUNG

HOSTINGER

NPRD-Anforderungsrichtlinie Datenschutzrichtlinie Rückerstattungsrichtlinie Nutzungsbedingungen

Und mehr

Die Preise sind ohne Mehrwertsteuer aufgeführt