DATENSCHUTZVEREINBARUNG VON CRITEO

PRÄAMBEL

Diese Datenschutzvereinbarung von Criteo (nachfolgend die „**DSV**“) ergänzt die Rahmennutzungsbedingungen von Criteo (die „**Nutzungsbedingungen**“) und die relevanten Spezifischen Nutzungsbedingungen von Criteo (die „S**pezifischen Bedingungen**“) oder jede andere anwendbare Vereinbarung mit dem Partner (zusammen, der „**Vertrag**“) und wird hiermit in den Vertrag zwischen Criteo und dem Partner für die Bereitstellung der entsprechenden Criteo-Services einbezogen.

Diese DSV beschreibt die Schutz- und Sicherheitsverpflichtungen der Parteien in Bezug auf die Verarbeitung personenbezogener Daten, die im Zusammenhang mit der Erbringung der betreffenden Criteo-Services erfolgt, einschließlich der Verarbeitung von Service-Daten, sofern und nur soweit diese Daten personenbezogene Daten enthalten, in Übereinstimmung mit den Anforderungen des Datenschutzrechts. Diese DSV ist in die folgenden Abschnitte unterteilt:

- **Abschnitt I: Allgemeine Bestimmungen**
  - Abschnitt I ist anwendbar, wenn der Partner Services von Criteo bestellt hat, unabhängig von der Art der Services.

- **Abschnitt II: Bedingungen für gemeinsam Verantwortliche**
  - Abschnitt II ist anwendbar, wenn der Partner Services bestellt hat, bei denen Criteo und der Partner als gemeinsame Verantwortliche handeln, wie in den jeweiligen Spezifischen Bedingungen dargelegt (die „**gemeinsam verantworteten Services**“).

- **Abschnitt III: Bedingungen zwischen Verantwortlichem und Auftragsverarbeiter (gilt nur für Mabaya)**
  - Abschnitt III ist anwendbar, wenn der Partner Services bestellt hat, bei denen der Partner als Verantwortlicher und Criteo als Auftragsverarbeiter fungiert und personenbezogene Daten im Auftrag des Partners verarbeitet, wie in den jeweiligen Spezifischen Bedingungen dargelegt (die „**Verantwortlicher-an-Auftragsverarbeiter-Services**“).

Abschnitt I dieser DSV gilt immer für die Parteien. Die Anwendung von Abschnitt II und/oder III hängt von dem Status ab, unter dem Criteo tätig ist und der in den Spezifischen Bedingungen oder in einer anderen anwendbaren Vereinbarung für den vom Partner bestellten Service festgelegt ist.

Abschnitt I: Allgemeine Bestimmungen

Die Bestimmungen dieses Abschnitts I „Allgemeine Bedingungen“ gelten immer dann, wenn der Partner Services von Criteo bestellt hat, unabhängig von der Art der bestellten Services.

1 Begriffsbestimmungen

Sofern hierin nicht anders angegeben, sind auf diese DSV die in dem Vertrag dargelegten Definitionen anwendbar. Die unten aufgeführten zusätzlichen Definitionen gelten für diese DSV.

„Einwilligung“	ist jede Willensbekundung der betroffenen Person, die aus freien Stücken, für den konkreten Fall, in Kenntnis der Sachlage und unmissverständlich erfolgt und mit der sie durch eine Erklärung oder eine eindeutige bestätigende Handlung ihr Einverständnis mit der Verarbeitung der sie betreffenden personenbezogenen Daten zum Ausdruck bringt.
„Verantwortlicher“	bezeichnet die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen die Zwecke und Mittel der Verarbeitung personenbezogener Daten bestimmt. Gemäß Abschnitt II dieser DSV fungieren Criteo S.A., als Muttergesellschaft der Criteo Gruppe, und der Partner als gemeinsame Verantwortliche und gemäß Abschnitt III dieser DSV fungiert der Partner als Verantwortlicher. Der Begriff „Verantwortlicher“ wird als „Business“ gemäß CPRA betrachtet.

„Datenschutzrecht“	bezeichnet alle anwendbaren internationalen, nationalen, bundesstaatlichen und einzelstaatlichen Gesetze und Verordnungen in Bezug auf Datenschutz und Privatsphäre, einschließlich, aber nicht beschränkt auf, (a) die Datenschutz-Grundverordnung („EU DSGVO“); (b) den „UK Data Protection Act“ („UK-GDPR“); (c) den „California Consumer Privacy Act“ („CCPA“) und der „California Privacy Rights Act“ („CPRA“); (d) den „Virginia Consumer Data Protection Act“ („VCDPA"); (e) den „Colorado Privacy Act“ („CPA“); (f) den „Connecticut Data Privacy Act“ („CTDPA“); (g) den „Utah Consumer Privacy Act“ („UCPA“); (h) den „Oregon Consumer Privacy Act“ („OCPA“); (i) den „Texas Data Privacy and Security Act” (TDPSA”); (j) den “Montana Consumer Data Privacy Act” (“MTCDPA”); (k) den koreanischen „Personal Information Protection Act“ („PIPA“); jeweils in der in jedem Land geltenden Fassung, sowie alle von Zeit zu Zeit geänderten oder ersetzenden Gesetze (oder ähnliche). Aus Gründen der Klarheit umfasst das Datenschutzrecht ebenfalls alle rechtlich bindenden Anforderungen, die von den zuständigen Datenschutzbehörden erlassen wurden (i) die Verarbeitung und Sicherheit von Informationen in Bezug auf natürliche Personen regeln und Regeln zum Schutz der Rechte und Freiheiten dieser natürlichen Personen in Bezug auf die Verarbeitung der sie betreffenden Daten vorsehen, (ii) Festlegung von Regeln zum Schutz der Privatsphäre in Bezug auf Datenverarbeitung und elektronische Kommunikation, oder (iii) Rechte für Personen zu erlassen, die gegenüber Organisationen in Bezug auf die Verarbeitung ihrer personenbezogenen Daten durchsetzbar sind, einschließlich des Auskunftsrechts, Berichtigung und Löschung. Die hier aufgeführten Datenschutzgesetze gelten für den Partner nur insoweit, als dies nach den gesetzlichen Kriterien vorgesehen ist.
„Betroffene Person“	ist eine bestimmbare natürliche Person, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennung (z. B. einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung) oder zu einem oder mehreren besonderen Merkmalen dieser natürlichen Person. Für die Zwecke dieser DSV bezieht sich „betroffene Person“ auf die natürlichen Personen, deren personenbezogene Daten im Rahmen der Bereitstellung der relevanten Criteo-Services verarbeitet werden.
„Gemeinsam Verantwortlicher“	bezeichnet einen Verantwortlichen, der gemeinsam mit einem oder mehreren anderen Verantwortlichen handelt. Gemäß Abschnitt II dieser DSV fungieren Criteo und der Partner als gemeinsame Verantwortliche.
„Personenbezogene Daten“	bezeichnet alle Informationen, die eine identifizierte oder identifizierbare natürliche Person oder einen Haushalt identifizieren, sich auf diese beziehen, diese beschreiben oder mit diesen in Verbindung gebracht werden können oder vernünftigerweise mit diesen in Verbindung gebracht werden können, die in Verbindung mit der Bereitstellung der relevanten Criteo-Services verarbeitet werden.
„Verletzung des Schutzes personenbezogener Daten“	bezeichnet eine Sicherheitsverletzung, die zur versehentlichen oder unrechtmäßigen Vernichtung, zum Verlust, zur Änderung, zur unbefugten Offenlegung oder zum unbefugten Zugriff auf übermittelte, gespeicherte oder anderweitig verarbeitete personenbezogene Daten führt.
„Auftragsverarbeiter“	bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Gemäß Abschnitt II dieser DSV sind die Auftragsverarbeiter, die entweder von Criteo oder dem Partner beauftragt werden können, Auftragsverarbeiter und gemäß Abschnitt III dieser DSV fungiert Criteo S.A. als Muttergesellschaft der Criteo Gruppe als Auftragsverarbeiter.
„Verarbeitung“	bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

„Regulierungsbehörde“	bezeichnet die zuständige Behörde oder Regierungsstelle, die für die Überwachung der Einhaltung des Datenschutzrechtes zuständig ist, einschließlich, aber nicht beschränkt auf: die französische CNIL (die Aufsichtsbehörde von Criteo), das UK Information Commissioner's Office, die California Privacy Protection Agency; oder die Generalstaatsanwälte der US-Bundesstaaten.

Die Begriffe „Business“, „**Geschäftszweck (Business Purpose)**“, „**Verkauf (Sale)**“, „**Dienstleister (Service Provider)**“ und „**Teilen (Share)**“ haben die gleiche Bedeutung wie im geltenden Datenschutzrecht, und ihre verwandten Begriffe sind entsprechend auszulegen.

2 Einhaltung von Gesetzen

2.1 Jede Partei erfüllt ihre jeweiligen Verpflichtungen gemäß dem anwendbaren Datenschutzrecht sowie dieser DSV und ist in der Lage, dies auch nachzuweisen.

2.2 Der Partner erkennt ausdrücklich an und erklärt sich damit einverstanden, dass seine Nutzung der gemeinsamen verantworteten Services und der Verantwortlicher-an-Auftragsverarbeiter-Services im Einklang mit dem Datenschutzrecht steht.

3 Autorisierung

3.1 Eine Partei darf personenbezogene Daten nicht der anderen Partei gegenüber offenlegen, es sei denn, die offenlegende Partei gewährleistet der anderen Partei, dass diese Offenlegung mit dem Datenschutzrecht übereinstimmt und dass sie alle geltenden Anforderungen an Informationen, Benachrichtigungen, Autorisierungen oder Einwilligungen der zuständigen öffentlichen Behörde(n) oder der relevanten betroffenen Personen in Bezug auf personenbezogene Daten, die die offenlegende Partei der anderen Partei zur Verfügung stellt, erfüllt hat. Jede offenlegende Partei muss für die Laufzeit des Vertrages Nachweise über die Einhaltung solcher Anforderungen aufbewahren und diese der anderen Partei auf Anfrage unverzüglich zur Verfügung stellen.

3.2 Nichts in dieser DSV verbietet oder beschränkt Criteos Rechte zur Implementierung der Anonymisierung personenbezogener Daten, die im Zusammenhang mit dem Vertrag verarbeitet werden, und der Partner autorisiert Criteo hiermit, Anonymisierungstechniken in Übereinstimmung mit dem Datenschutzrecht zu implementieren, soweit dies nach dem Datenschutzrecht erforderlich ist. Das heißt, Daten, die aus einer wirksamen und gesetzeskonformen Anonymisierung resultieren, fallen nicht unter diese DSV und generell nicht unter das Datenschutzrecht.

4 Zusammenarbeit

4.1 Die Parteien müssen miteinander kooperieren, um das einschlägige Datenschutzrecht zu befolgen und ihre Pflichten aus dem anwendbaren Datenschutzrecht sowie dieser DSV zu erfüllen.

4.2 Die Parteien führen eine angemessene Dokumentation über die von ihnen durchgeführten Verarbeitungsaktivitäten und über ihre Einhaltung des Datenschutzrechts und dieser DSV in Bezug auf die gemeinsam verantworteten Services und die Verantwortlicher-an-Auftragsverarbeiter-Services.

4.3 Im Falle einer Ermittlung, eines Verfahrens, einer formellen Anfrage nach Informationen oder Dokumentation oder eines ähnlichen Ereignisses in Verbindung mit einer Datenschutzbehörde und in Bezug auf die gemeinsam verantworteten Services und die Verantwortlicher-an-Auftragsverarbeiter-Services oder auf personenbezogene Daten werden die Parteien unverzüglich und angemessen Anfragen der anderen Partei bearbeiten, die sich auf die Verarbeitung personenbezogener Daten im Rahmen des Vertrages beziehen.

4.4 Im Falle einer Änderung oder eines neuen Datenschutzrechts werden sich die Parteien einvernehmlich auf alle vernünftigerweise erforderlichen Änderungen oder Überarbeitungen dieser DSV einigen.

5 Datenschutzbeauftragte

5.1 Criteo und der Partner haben einen Datenschutzbeauftragten ernannt. Der Datenschutzbeauftragte von Criteo ist erreichbar unter: dpo@criteo.com. Die Kontaktdaten des Datenschutzbeauftragten des Partners müssen Criteo unverzüglich mitgeteilt werden.

Abschnitt II – Bedingungen für gemeinsam Verantwortliche

6 Anwendungsbereich dieses Abschnitts II

6.1 Dieser Abschnitt II ist nur auf die Verarbeitung personenbezogener Daten anwendbar, die im Rahmen der Bereitstellung der vom Partner bestellten gemeinsam verantworteten Services durch Criteo durchgeführt wird.

6.2 Gemäß Artikel 26 DSGVO legen die Parteien hiermit ihre jeweiligen Verantwortlichkeiten für die Einhaltung ihrer Verpflichtungen gemäß der DSGVO fest.

6.3 Für die Zwecke der CPRA ist der Partner ein „Business" und Criteo ist ein „Dritter".

7 Pflichten der Parteien bei ihrer Tätigkeit als gemeinsam Verantwortliche

7.1 Bei der Verarbeitung personenbezogener Daten als gemeinsam Verantwortliche gemäß Abschnitt II dieser DSV erklärt sich jede Partei damit einverstanden, dass sie:

(a) die sich aus dem Datenschutzrecht ergebenden Anforderungen erfüllt und die Verpflichtungen aus dieser DSV weder so erfüllt, dass der andere gemeinsame Verantwortliche seine sich aus dem Datenschutzrecht ergebenden Verpflichtungen verletzt, noch fordert sie den anderen gemeinsamen Verantwortlichen dazu auf, seine Verpflichtungen so zu erfüllen, dass der gemeinsame Verantwortliche seine Verpflichtungen aus dem Datenschutzrecht verletzt.

(b) alle im Datenschutzrecht vorgesehenen Datenschutzgrundsätze berücksichtigen, einschließlich, aber nicht beschränkt auf die Grundsätze der Zweckbindung, Datenminimierung, Genauigkeit, Speicherbegrenzung, Sicherheit, Integrität und Vertraulichkeit, Transparenz und des Schutzes personenbezogener Daten durch Design und Standards.

(c) Aufzeichnungen über die Verarbeitung der personenbezogenen Daten unter ihrer Verantwortung führen.

(d) angemessene technische und organisatorische Maßnahmen ergreifen, um ein Sicherheitsniveau zu gewährleisten, das den Risiken entspricht, die durch die Verarbeitung der von ihr durchgeführten Verarbeitung personenbezogenen Daten entstehen (einschließlich, für den Partner, in Bezug auf die digitale Fläche des Partners), insbesondere um die personenbezogenen Daten vor versehentlicher oder unrechtmäßiger Zerstörung oder versehentlichem Verlust, Änderung, unbefugter Offenlegung oder Zugriff zu schützen.

(e) alle erforderlichen Maßnahmen ergreifen, um eine Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den von ihren jeweils verarbeiteten personenbezogenen Daten zu beheben, die Auswirkungen mildern, eine weitere Verletzung des Schutzes personenbezogener Daten zu verhindern und, falls erforderlich, die zuständige(n) Datenschutzbehörde(n) und die betroffenen Personen benachrichtigen.

(f) bei der Erstellung der erforderlichen Datenschutz-Folgenabschätzungen mitwirken.

(g) jede Bewertung, Konsultation und/oder Benachrichtigung der zuständigen Datenschutzbehörden oder betroffenen Personen in Bezug auf durch die jeweilige Partei durchgeführte Verarbeitung erfolgt; und

(h) sie Anfragen und/oder Beschwerden von betroffenen Personen, insbesondere die Anfragen in Bezug auf die Ausübung von deren Rechte gemäß dem Datenschutzrecht, einschließlich der Auskunftsrechte, Berichtigung, Löschung und Widerspruch sowie das Recht auf Widerruf der Einwilligung, bearbeiten. Wenn eine Partei eine Anfrage einer betroffenen Person in Bezug auf personenbezogene Daten erhält, die von der anderen Partei verarbeitet werden, wird diese empfangende Partei die betroffene Person auf die Datenschutzrichtlinie der anderen Partei verweisen, die erklärt, wie sie ihre Anfrage bei der anderen Partei einreichen kann, um es dieser anderen Partei zu ermöglichen, direkt auf die Anfrage der betroffenen Person zu antworten.

8 Criteos Verpflichtungen

8.1 Criteo ist in Übereinstimmung mit und in dem Umfang, der durch das Datenschutzrecht vorgeschrieben ist, allein dafür verantwortlich, einen Link zur Datenschutzrichtlinie-Seite von Criteo (www.criteo.com/privacy) aufzunehmen, der

Informationen für betroffene Personen darüber enthält, wie der Criteo-Service in allen auf den digitalen Flächen des Partners geschalteten Anzeigen deaktiviert werden kann (und einen „Opt-out“-Link einzufügen).

8.2 Soweit Criteo eine "Third Party" im Sinne des CPRA ist: (a) Die Verwendung personenbezogener Daten durch Criteo ist auf die im Vertrag genannten spezifischen Zwecke beschränkt, und Criteo darf über diese spezifischen Zwecke nicht hinausgehen; (b) Criteo muss die geltenden Verpflichtungen einhalten und das gleiche Maß an Datenschutz bieten, das von einem Business gemäß dem CPRA in Bezug auf personenbezogene Daten verlangt wird; (c) Criteo räumt dem Partner das Recht ein, nach angemessener Ankündigung entsprechende Maßnahmen zu ergreifen, um sicherzustellen, dass Criteo personenbezogene Daten in Übereinstimmung mit diesem Vertrag und den geltenden Datenschutzrechten verwendet, einschließlich angemessener und geeigneter Maßnahmen, um die unbefugte Verwendung personenbezogener Daten zu unterbinden und zu beheben; und (d) Criteo benachrichtigt den Partner, wenn es feststellt, dass es seine Verpflichtungen gemäß den geltenden Datenschutzrechten nicht mehr erfüllen kann.

9 Pflichten des Partners

9.1 Der Partner ist in Übereinstimmung mit und im vom Datenschutzrecht geforderten Umfang allein verantwortlich für:

(a) die Bereitstellung aller erforderlichen Informationen an die betroffenen Personen gemäß dem Datenschutzrecht, einschließlich in Übereinstimmung mit den Artikeln 13 und 14 der DSGVO, in Bezug auf die Verarbeitung der personenbezogenen Daten in Bezug auf die gemeinsam verantworteten Services;

(b) die Bereitstellung eines angemessenen Hinweises in den digitalen Flächen des Partners für jede relevante Verarbeitung personenbezogener Daten durch Criteo für die gemeinsam verantworteten Services, einschließlich der Bereitstellung eines Links zu den Datenschutzrichtlinien von Criteo (www.criteo.com/privacy);

(c) die Einholung und Dokumentation von Einwilligungs- oder Opt-Out-Erklärungen, die gegebenenfalls von betroffenen Personen erteilt wurden;

(d) die Umsetzung von Auswahlmechanismen, um eine gültige Einwilligung von betroffenen Personen oder Opt-Out-Erklärung, sofern anwendbar, in Übereinstimmung mit dem Datenschutzrecht und gegebenenfalls mit den spezifischen Anforderungen der zuständigen lokalen Aufsichtsbehörden einzuholen;

(e) wo Opt-Out-Erklärungen anwendbar sind, den betroffenen Personen das Recht einzuräumen, dem Verkauf und der Weitergabe ihrer personenbezogenen Daten oder der Verwendung der personenbezogenen Daten für Zwecke der gezielten Werbung zu widersprechen;

(f) die Einhaltung der für die Gültigkeitsdauer der eingeholten Einwilligung geltenden Anforderungen und die Anforderung der Einwilligung der betroffenen Personen nach Ablauf dieser Gültigkeitsdauer;

(g) falls zutreffend, sichert der Partner zu und gewährleistet, dass jeder dritte Werbetechnologiepartner, mit dem der Partner in Bezug auf die Werbefläche auf den digitalen Flächen zusammenarbeitet, die über die Criteo-Plattform zum Verkauf angeboten wird (jeweils ein „Consented Third-party Vendor"), die Bestimmungen dieser DSV vollständig einhält;

(h) auf Anfrage und jederzeit unverzüglich den Nachweis zu erbringen, dass der Partner die Einwilligung einer betroffenen Person eingeholt hat.

Abschnitt III – Verantwortlicher-an-Auftragsverarbeiter- Bedingungen (gilt nur für Mabaya)

10 Anwendungsbereich dieses Abschnitts III

10.1 Dieser Abschnitt III ist nur in Bezug auf die Verarbeitung personenbezogener Daten anwendbar, die der Partner als Verantwortlicher oder Business (je nach Fall) in Auftrag gegeben hat und für die im Zusammenhang mit Verantwortlicher-an-Auftragsverarbeiter-Services durchgeführt wird, für die Criteo als Auftragsverarbeiter oder Dienstleister (Service Provider) (je nach Anwendungsfall) fungiert, und deren Gegenstand, Art und Zweck, und die Art der personenbezogenen Daten, die Kategorien der betroffenen Personen und die Dauer der Verarbeitung in Anhang 1 „Verantwortlicher-an-Auftragsverarbeiter-Services – Einzelheiten zur Verarbeitung personenbezogener Daten“ dargelegt sind.

11 Pflichten des Partners

11.1 Der Partner darf Criteo keine personenbezogenen Daten zur Verfügung stellen, es sei denn, dies ist für die Erbringung der Criteo-Services erforderlich und der Partner hat in jedem Fall die erforderlichen Mitteilungen gemacht und die erforderlichen Einwilligungen der betroffenen Personen eingeholt, deren personenbezogene Daten von Criteo gemäß des Vertrages verarbeitet werden. Der Partner ist verpflichtet, bei der Nutzung der Criteo-Services personenbezogene Daten in Übereinstimmung mit den Anforderungen des Datenschutzrechtes zu verarbeiten und Criteo unverzüglich zu benachrichtigen, wenn der Partner gegen ein Datenschutzrecht verstößt. Die Anweisungen des Partners an Criteo in Bezug auf die Verarbeitung personenbezogener Daten müssen dem Datenschutzrecht entsprechen. Der Partner ist allein dafür verantwortlich, die Richtigkeit, Rechtmäßigkeit und Qualität der personenbezogenen Daten sicherzustellen und sicherzustellen, dass die Criteo anvertraute Verarbeitung eine angemessene Rechtsgrundlage gemäß des Datenschutzrechts hat.

12 Criteos Pflichten

12.1 **Anweisungen für Partner.** Criteo verarbeitet personenbezogene Daten für die relevanten Verantwortlicher-an-Auftragsverarbeiter-Services nur auf dokumentierte Anweisung des Partners hin. Der Partner darf Criteo nicht anweisen, personenbezogene Daten auf eine Weise zu verarbeiten, die nicht mit dem Vertrag und insbesondere dieser DSV vereinbar ist. Criteo informiert den Partner unverzüglich, wenn Criteo vernünftigerweise der Ansicht ist, dass es nicht in der Lage ist, die Anweisungen des Partners zu befolgen, oder wenn diese Anweisungen nicht mit den Spezifischen Bedingungen oder allgemeiner mit dem Vertrag kompatibel sind.

12.2 **Unrichtige oder veraltete Daten.** Criteo informiert den Partner, wenn Criteo Kenntnis davon erhält, dass die personenbezogenen Daten unrichtig oder veraltet sind, und Criteo kooperiert auf Anfrage mit dem Partner, um diese Daten zu löschen oder zu korrigieren.

12.3 **Verarbeitung personenbezogener Daten.** Soweit dies nach geltendem Datenschutzrecht erforderlich ist, wird der Partner Criteo nur anweisen, personenbezogene Daten für diejenigen Geschäftszwecke (Business Purposes) zu verarbeiten, die nach geltendem Datenschutzrecht zulässig sind, und er wird Criteo personenbezogene Daten nur für die begrenzten und festgelegten Zwecke offenlegen, die im Vertrag angegeben sind. Der Partner behält sich das Recht vor, nach angemessener Ankündigung angemessene und geeignete Schritte zu unternehmen, um sicherzustellen, dass Criteo die übermittelten personenbezogenen Daten in einer Weise verwendet, die mit den Verpflichtungen des Partners nach dem geltenden Datenschutzrecht vereinbar ist, einschließlich angemessener und geeigneter Schritte, um die unbefugte Verwendung personenbezogener Daten zu unterbinden und zu beheben.

Criteo ist nicht berechtigt: (a) personenbezogene Daten zu Verkaufen oder zu Teilen ; (b) personenbezogene Daten für andere Zwecke als die im Vertrag festgelegten Geschäftszwecke zu speichern, zu verwenden oder offenzulegen; (c) personenbezogene Daten außerhalb der direkten Geschäftsbeziehung zwischen dem Partner und Criteo zu speichern, zu verwenden oder offenzulegen; oder (d) personenbezogene Daten, die es vom Partner erhält, mit personenbezogenen Daten zu kombinieren, die es von oder im Namen einer oder mehrerer anderer Personen erhält oder die es aus seiner eigenen Interaktion mit betroffenen Personen erhebt, vorausgesetzt, dass Criteo personenbezogene Daten kombinieren darf, um einen Geschäftszweck zu erfüllen (mit Ausnahme von „Werbe- und Marketingdienstleistungen“, wie unter geltendem Datenschutzrecht definiert). Criteo erfüllt die geltenden Verpflichtungen und bietet das gleiche Maß an Datenschutz, wie es das geltende Datenschutzrecht vorschreibt, und unterstützt den Partner durch geeignete technische und organisatorische Maßnahmen bei der Einhaltung der datenschutzrechtlichen Anforderungen, wobei die Art der Verarbeitung berücksichtigt wird. Criteo benachrichtigt den Partner, wenn es feststellt, dass es seinen Verpflichtungen gemäß dem geltenden Datenschutzrecht nicht mehr nachkommen kann.

12.4 **Technische und organisatorische Maßnahmen.** Criteo wird geeignete technische und organisatorische Maßnahmen ergreifen, um die Sicherheit der personenbezogenen Daten zu gewährleisten, einschließlich des Schutzes vor einer Verletzung des Schutzes personenbezogener Daten. Criteo wird bei der Erfüllung seiner Verpflichtungen aus diesem Absatz zumindest die in Anhang 2 „Criteo-Sicherheitsplan“ genannten technischen und organisatorischen Maßnahmen umsetzen”. Der Partner bestätigt Criteo hiermit, dass er der Ansicht ist, dass die technischen und organisatorischen Maßnahmen von Criteo, wie diese in Anhang 2 „Criteo-Sicherheitsplan“ angegeben sind, ein angemessenes Sicherheitsniveau bieten. Criteo unterstützt den Partner auch bei der Erfüllung seiner Verpflichtungen in Bezug auf die Sicherheit der Verarbeitung personenbezogener Daten, einschließlich gemäß Artikel 32 der DSGVO.

12.5 **Verletzung des Schutzes personenbezogener Daten.** Im Falle einer Verletzung des Schutzes personenbezogener Daten in Bezug auf personenbezogene Daten, die von Criteo verarbeitet werden, wird Criteo angemessene Maßnahmen ergreifen, um die Verletzung zu beheben, einschließlich von Maßnahmen zur Minderung ihrer nachteiligen Auswirkungen. Criteo benachrichtigt den Partner außerdem unverzüglich, nachdem es von der Verletzung Kenntnis erlangt hat, und gewährt ihm die für die Bereitstellung relevanter Informationen erforderliche Zeit, einschließlich z. B. einer Beschreibung der Art der Verletzung (einschließlich, soweit möglich, der Kategorien und der ungefähren Anzahl der betroffenen Personen und personenbezogenen Datensätze), ihrer wahrscheinlichen Folgen und der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung, einschließlich gegebenenfalls Maßnahmen zur Abschwächung ihrer möglichen nachteiligen Auswirkungen. Im Falle einer Verletzung des Schutzes personenbezogener Daten, die sich auf von Criteo verarbeitete personenbezogene Daten bezieht, ist der Partner allein für die Benachrichtigung der betroffenen Personen und/oder der Regulierungsbehörden verantwortlich, wie es das Datenschutzrecht vorschreibt, und Criteo arbeitet mit dem Partner zusammen und unterstützt ihn, damit er allen Aufforderungen einer zuständigen Behörde und/oder der betroffenen Personen nachkommen kann, wobei die Art der Verarbeitung und die Criteo zur Verfügung stehenden Informationen berücksichtigt werden. Bevor eine solche Benachrichtigung erfolgt, muss der Partner Criteo konsultieren und ihm die Möglichkeit geben, zu einer Benachrichtigung im Zusammenhang mit einer Verletzung des Schutzes personenbezogener Daten Stellung zu nehmen. Keine Bestimmung dieser DSV ist so auszulegen, dass sie Criteo dazu verpflichtet, gesetzliche Verpflichtungen zu verletzen oder deren Einhaltung zu verzögern, die es in Bezug auf einen Verstoß gegen personenbezogene Daten hat. Criteo haftet nicht für die in diesem Abschnitt beschriebenen Verpflichtungen zur Verwaltung und Benachrichtigung bei Verstößen gegen personenbezogene Daten, es sei denn, der Verstoß gegen personenbezogene Daten wird durch einen Verstoß von Criteo gegen die Sicherheitsverpflichtungen gemäß Abschnitt 12.4 dieser DSGVO oder eine andere Verletzung des Datenschutzrechts durch Criteo verursacht.

12.6 **Zugriff auf personenbezogene Daten.** Criteo gewährt seinen Mitarbeitern nur insoweit Zugang zu den personenbezogenen Daten, als dies für die Durchführung, Verwaltung und Überwachung des Vertrages und in Übereinstimmung mit dieser DSV unbedingt erforderlich ist. Criteo hat sicherzustellen, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen einer oder mehrere Vertraulichkeitsvereinbarungen verpflichtet haben oder einer angemessenen gesetzlichen Vertraulichkeitsverpflichtung unterliegen.

13 **Rechte der betroffenen Personen.** Soweit gesetzlich zulässig, wird Criteo den Partner unverzüglich über jede Anfrage informieren, die es von einer betroffenen Person erhalten hat, um die Rechte der betroffenen Person auszuüben, einschließlich der Rechte auf: Kenntnisnahme/Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch, Datenübertragbarkeit, Widerspruch gegen (opt out) die Verarbeitung und/oder den Verkauf (Sale) oder die Weitergabe personenbezogener Daten, Einschränkung der Nutzung oder Offenlegung sensibler personenbezogener Daten oder jeden anderen Antrag in Bezug auf personenbezogene Daten der betroffenen Person, wie im geltenden Datenschutzrecht festgelegt. Criteo wird auf die Anfrage nicht selbst antworten. Criteo unterstützt den Partner in angemessener Weise durch die Umsetzung geeigneter technischer und organisatorischer Maßnahmen, soweit dies möglich ist, bei der Erfüllung seiner Verpflichtungen zur Beantwortung von Anträgen der betroffenen Personen auf Ausübung ihrer Rechte nach dem Datenschutzrecht, wobei die Art der Verarbeitung zu berücksichtigen ist. Soweit gesetzlich zulässig, ist der Partner für alle Kosten verantwortlich, die durch die Bereitstellung einer solchen Unterstützung durch Criteo entstehen. Nichts in diesem Abschnitt 13 erfordert, dass Criteo Geschäftsgeheimnisse offenlegt oder aufdeckt.

13.1 **Datenschutz-Folgenabschätzung.** Auf Anfrage des Partners, auf dessen Kosten und in dem nach dem Datenschutzrecht erforderlichen Umfang unterstützt Criteo den Partner bei der Durchführung einer erforderlichen Datenschutz-Folgenabschätzung auf Anfrage des Partners unter Berücksichtigung der Criteo vorliegenden Informationen. Soweit dies nach der Datenschutz-Grundverordnung (DSGVO) oder der britischen Datenschutz-Grundverordnung (UK-DSGVO) erforderlich ist, unterstützt Criteo den Partner in angemessener Weise bei seiner Zusammenarbeit oder vorherigen Konsultation mit einer Regulierungsbehörde bei der Erfüllung seiner Aufgaben im Zusammenhang mit diesem Abschnitt 13.1.

13.2 **Unterauftragsverarbeiter.** Criteo kann Unterauftragsverarbeiter beauftragen, wie dies in Anhang 1 „Verantwortlicher-an-Auftragsverarbeiter-Services – Einzelheiten zur Verarbeitung personenbezogener Daten“ dargelegt ist. Der Partner erteilt Criteo die allgemeine Erlaubnis, andere Unterauftragsverarbeiter mit der Durchführung der Verarbeitung für die entsprechenden Services des für die Verarbeitung Verantwortlichen zu beauftragen. Auf schriftliche Anfrage des Partners informiert Criteo den Partner über alle Änderungen bezüglich der Hinzufügung oder des Austauschs von Unterauftragsverarbeitern. Wenn der Partner innerhalb von dreißig (30) Tagen nach der Mitteilung von Criteo an den

Partner aus berechtigten Gründen [bezüglich des Datenschutzes] gegen diese Änderungen Einspruch erhebt, werden die Parteien nach Treu und Glauben diskutieren, um eine für beide Seiten akzeptable Lösung zu finden. Wenn sich die Parteien nicht einigen, kann Criteo den Vertrag ganz oder teilweise nur in Bezug auf die betroffenen Verantwortlicher-an-Auftragsverarbeiter-Services kündigen. Bei der Beauftragung eines anderen Auftragsverarbeiters schließt Criteo eine Vereinbarung ab, die für diesen Auftragsverarbeiter verbindlich ist und in der die gleichen oder strengere Datenschutzverpflichtungen wie in dieser DSGVO festgelegt sind, wobei insbesondere ausreichende Garantien für die Umsetzung ähnlicher technischer und organisatorischer Maßnahmen gegeben werden.

13.3 **Verarbeitung personenbezogener Daten außerhalb der Anweisungen des Partners.** Ungeachtet des Vorstehenden hat Criteo den Partner zu informieren, sofern das anwendbare Recht oder eine verbindliche Entscheidung einer zuständigen Behörde Criteo verpflichtet, personenbezogene Daten für die Zwecke der Bereitstellung der Verantwortlicher-an-Auftragsverarbeiter-Services außerhalb der Anweisungen des Partners zu verarbeiten, sofern dies nicht auf Basis des anwendbaren Rechts verboten ist.

13.4 **Prüfung.** Der Partner kann in angemessenen Abständen schriftlich verlangen, dass Criteo dem Partner Informationen über die Einhaltung seiner Verpflichtungen gemäß Abschnitt III dieser DSV in Form einer Kopie der zu diesem Zeitpunkt aktuellen Prüfungen oder Zertifizierungen Criteos durch Dritte zur Verfügung stellt.

Der Partner kann eine Vor-Ort-Prüfung der in Abschnitt III dieser DSV beschriebenen Verarbeitungsaktivitäten von Criteo beantragen, indem er Criteo eine Benachrichtigung mit angemessener Vorankündigung zukommen lässt. Eine solche Vor-Ort-Prüfung darf nur durchgeführt werden, wenn (i) die von Criteo wie oben dargelegt zur Verfügung gestellten Informationen unzureichend sind, (ii) eine Verletzung des Schutzes personenbezogener Daten aufgetreten ist oder (iii) eine solche Prüfung durch das Datenschutzrecht vorgeschrieben ist oder durch eine zuständige Regulierungsbehörde angeordnet wurde.

Die Parteien einigen sich über Umfang, Zeitpunkt und Dauer der Prüfung. Die Prüfung darf die Aktivitäten von Criteo nicht unangemessen beeinträchtigen.

Der Partner darf nur einen externen Wirtschaftsprüfer ernennen, der kein Wettbewerber von Criteo ist. Ein solcher externer Wirtschaftsprüfer hat vor der Durchführung der Prüfung eine Geheimhaltungsvereinbarung mit Criteo und dem Partner abzuschließen.

Nach der Vor-Ort-Prüfung hat der Partner Criteo unverzüglich die Ergebnisse dieser Prüfung mitzuteilen.

Die Parteien haben den Regulierungsbehörden auf Anfrage die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, zur Verfügung zu stellen.

Der Partner trägt alle Kosten im Zusammenhang mit Prüfungen.

13.5 **Übermittlung personenbezogener Daten.** Jede Übermittlung von Daten an ein Drittland oder eine internationale Organisation durch Criteo erfolgt nur auf der Grundlage dokumentierter Anweisungen des Partners in Übereinstimmung mit Kapitel V der DSGVO. Der Partner erklärt sich damit einverstanden, dass, wenn Criteo einen Unterauftragsverarbeiter gemäß Klausel 13.2 mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Partners) beauftragt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der DSGVO beinhalten, Criteo und der Unterauftragsverarbeiter die Einhaltung des Kapitels V der DSGVO sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Europäischen Kommission gemäß Artikel 46(2) DSGVO verabschiedet wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

13.6 **Folgen der Kündigung.** Wenn der Partner einen Verantwortlicher-an-Auftragsverarbeiter-Service kündigt oder wenn der Vertrag aus irgendeinem Grund abläuft oder endet, wird Criteo nach Wahl des Partners alle personenbezogenen Daten, die nur für diesen Verantwortlicher-an-Auftragsverarbeiter-Service verarbeitet werden, löschen oder alle diese personenbezogenen Daten an den Partner zurückgeben. Criteo muss gegebenenfalls auf die schriftliche Anfrage des Partners hin eine Bestätigung vorlegen, dass Kopien dieser personenbezogenen Daten gelöscht wurden, unbeschadet etwaiger betrieblicher Backups, die von Criteo für einen angemessenen Zeitraum gemäß den Industriestandards aufbewahrt werden. Falls das anwendbare Recht Criteo die Löschung der personenbezogenen Daten verbietet, garantiert Criteo, dass es weiterhin die Einhaltung dieser DSV gewährleistet und diese personenbezogenen Daten nur in dem Umfang und so lange verarbeitet, wie es das anwendbare Recht verlangt.

Die bevollmächtigten Unterzeichner der Parteien haben diese DSV ordnungsgemäß unterzeichnet:

PARTNER	**CRITEO**
Unterschrift: _____	Unterschrift: _____
Name: _____	Name: _____
Titel: _____	Titel: _____
Datum: _____	Datum: _____

ANHANG 1: Verantwortlicher-an-Auftragsverarbeiter-Services – Einzelheiten zur Verarbeitung personenbezogener Daten

(gilt nur für Mabaya)

<table>
<tr><th colspan="4">Kategorie betroffener Personen</th></tr>
<tr><td>Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden</td><td>Nutzer der digitalen Flächen des Partners (Einkäufer)</td><td>Mitarbeiter des Verantwortlichen</td><td>Verkäufer (Mitarbeiter/Vertreter)</td></tr>
<tr><td>Kategorien der verarbeiteten personenbezogenen Daten</td><td>Kennungen, die aus einer Reihe von Zeichen bestehen (in einem Cookie oder anderweitig enthaltene Kennung), die vom Verantwortlichen bereitgestellt werden (wenn diese Daten gemäß dem Datenschutzrecht als personenbezogene Daten gelten)</td><td>Name und E-Mail-Adressen autorisierter Mitarbeiter/Vertreter des Verantwortlichen</td><td>E-Mail-Adressen von Verkäufern (um ihnen Berichte und Benachrichtigungen zu senden)</td></tr>
<tr><td>Sensible Daten</td><td colspan="3">N.Z.</td></tr>
<tr><td>Art der Verarbeitung</td><td colspan="3">Erfassung, Hosting, Verarbeitung zur Erbringung des Services, Löschung</td></tr>
<tr><td rowspan="2">Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden</td><td rowspan="2">Abgleich von Konversionen mit Klicks (im Kontext der Anzeigen)</td><td colspan="2">Identitätsprüfungen (Anmeldeseite)
Kontoverwaltung</td></tr>
<tr><td>E-Mail-Benachrichtigung an Verkäufer</td></tr>
<tr><td>Dauer der Verarbeitung</td><td colspan="3">Laufzeit des Vertrages</td></tr>
</table>

Der Partner erkennt an, dass Criteo die folgenden Unternehmen als Unterauftragsverarbeiter in Bezug auf die entsprechenden Verantwortlicher-an-Auftragsverarbeiter-Services einsetzt, und genehmigt dies:

Unterauftragsverarbeiter	**Gegenstand der Verarbeitung**	**Art der Verarbeitung**	**Kategorien betroffener Personen**	**Kategorien der verarbeiteten personenbezogenen Daten**	**Dauer der Verarbeitung**
Amazon Web Services (AWS)	Hosting (Rechenzentrum in Irland)	Hosting	Siehe oben	Siehe oben	Laufzeit des Vertrages

Sendgrid	Versenden von E-Mails an Kunden (USA)	Kontaktdaten zum Versenden von E-Mails verwenden	Mitarbeiter des Partners	E-Mail-Adressen	Laufzeit des Vertrages

ANHANG 2: Criteo-Sicherheitsplan

Dieser Sicherheitsplan (der „**Plan**“) stellt Sicherheitskontrollen in Bezug auf den/die Criteo-Service(s) und die gesamte Sicherheits-Governance dar.

Dieser Plan ergänzt die Bedingungen zwischen Criteo und dem Partner und ist Teil des Vertrages. Im Falle von Widersprüchen zwischen dem Vertrag und diesem Plan hat dieser Plan Vorrang.

1. **Begriffsbestimmungen**

Die folgenden Definitionen unterstützen die in diesem Plan angegebenen Bestimmungen:

Vertrauliche Informationen: bezeichnet, insbesondere im Zusammenhang mit diesem Plan, Informationen, die von Partnern und Criteo verarbeitet, gespeichert und von Criteo-Dienstplattformen übertragen werden, sowie damit verbundene Datenbestände und unterstützende Sicherheitskontrollen, die zum Schutz der Datensicherheit angewendet werden.

Datenbestände: bezeichnet alle Technologieplattformen, Komponenten, Daten oder Informationen, die über Criteo-Serviceproduktplattformen verarbeitet werden die vertrauliche Informationen verarbeiten, übermitteln oder speichern.

Datenschutzverletzung: bezeichnet eine Sicherheitsverletzung, die zur versehentlichen oder unrechtmäßigen Vernichtung, zum Verlust, zur Änderung, zur unbefugten Offenlegung oder zum unbefugten Zugriff auf übermittelte, gespeicherte oder anderweitig verarbeitete personenbezogene Daten führt.

Sicherheitsverletzung: bezeichnet jeden tatsächlichen oder potenziellen unbefugten Zugriff auf oder die Verwendung, Offenlegung, Änderung oder Zerstörung vertraulicher Informationen oder jede Handlung oder Unterlassung, die Daten, die für die Vertrags-Services relevant sind, gefährdet, die sich auf den Schutz der Sicherheit, Vertraulichkeit oder Integrität vertraulicher Informationen beziehen.

2. **Sicherheitskontrollen**

Die folgenden Sicherheits- und Datenschutzkontrollen werden von Criteo im Zusammenhang mit den Criteo-Services aufrechterhalten und unterstützt:

Sicherheits-Governance und -Management: Criteo unterhält ein Sicherheitsmanagementsystem, das der ISO 27002 ähnelt, einschließlich anderer branchenweit bekannter bewährter Praktiken für Datenschutz und Sicherheit sowie der Unterstützung von Sicherheitskontrollen. Dies beinhaltet eine angemessene Dokumentation (Sicherheitsrichtlinien, Prozesse, Richtlinien, Standards, Konfigurationsstandards und zugehörige Sicherheitskontrollen), um einen angemessenen Schutz der Datenbestände von Criteo und Partnern während des gesamten Lebenszyklus der Services zu gewährleisten.

Sicherheitsabschätzungen: Höchstens einmal pro Kalenderjahr und nur nach Erhalt einer schriftlichen Anfrage mit einer Vorankündigung von mindestens dreißig (30) Werktagen ist es dem Partner gestattet, Sicherheitsabschätzungen des Sicherheitsmanagementsystems von Criteo und der damit verbundenen Sicherheitskontrollen durchzuführen, die direkt mit den als Auftragsverarbeiter erbrachten Services verbunden sind. Die Sicherheitsbewertungen beschränken sich auf allgemeine detaillierte Sicherheitsfragebögen, Abfragen oder spezifische Fragen im Zusammenhang mit den vertraglich vereinbarten Dienstleistungen und schließen physische Audits, Penetrationstests, Scans oder andere eingreifende Aktivitäten aus. Die Sicherheitsabschätzungen sollten vorzugsweise von einem externen Prüfer durchgeführt werden, der der Vertraulichkeit unterliegt und Criteo seinen Bericht zur Validierung vorlegt, bevor die endgültigen Ergebnisse dem Partner zur Verfügung gestellt werden. Solche Anfragen werden umgehend unterstützt, indem der Zugriff auf die Sicherheitskontrollen von Criteo gewährt wird,

die zum Schutz der Datenbestände von Criteo und Partnern vor Sicherheitsbedrohungen, Risiken und Schwachstellen eingesetzt werden, wobei die Antworten innerhalb eines angemessenen Zeitrahmens bereitgestellt und genau dargestellt werden.

Sicherheit durch Dritte: Criteo unterhält angemessene Sicherheitskontrollen, um die Datensicherheitsrisiken für Services von Drittpartnern angemessen zu verwalten, um den Schutz der Daten von Criteo und Partnern zu gewährleisten.

Sicherheitsschulung: Criteo unterhält angemessene Programme zur Sensibilisierung für Sicherheit und Datenschutz, um die Datenbestände von Criteo und Partnern proaktiv zu schützen, und zwar mit Inhalten, die sich an den besten Praktiken der Branche orientieren, um die Risiken für die Datensicherheit zu mindern.

Physische und umgebungsbezogene Sicherheitskontrollen: Criteo unterhält angemessene physische und umgebungsbezogene Sicherheitskontrollen zum Schutz vor Datensicherheitsrisiken, zum Schutz vor Risiken für die Vertraulichkeit, Integrität und Verfügbarkeit. Alle diese Kontrollen werden an den geltenden branchenüblichen, betrieblichen und sicherheitsrelevanten Best Practices zum Schutz vor physischen und umweltbedingten Sicherheitsrisiken ausgerichtet, einschließlich physischer Zugangskontrollen, physischer Sicherheitsüberwachung und umweltbedingter Schutzmaßnahmen gegen Stromausfälle, Brandgefahren und damit verbundene betriebliche Risiken.

Zugriffskontrolle: Criteo unterhält ein umfassendes System zur Verwaltung der Zugriffskontrolle, das sich an den besten Praktiken der Branche orientiert, um die Datenbestände von Criteo und der Kunden zu schützen und eine angemessene Kontrolle des Zugriffs zu gewährleisten. Diese Kontrollen umfassen die Identifizierung von privilegierten Konten mit geeigneter Multifaktor-Authentifizierung (MFA), die auf Berechtigungen mit Zugriff auf vertrauliche Sicherheitsinformationen angewendet wird. Für alle autorisierten Konten, ob allgemein oder administrativ, werden Zugriffsprotokolle erfasst, überwacht und die Berechtigungen regelmäßig überprüft.

BCM-System (Business Continuity Management): Criteo führt ein Business Continuity Management („BCM“) System, in dem Kontinuitätskontrollen, Rollen, Verantwortlichkeiten und Wiederherstellungsmaßnahmen detailliert beschrieben werden, um die Anforderungen an die Verfügbarkeit der vertraglich vereinbarten Services als Reaktion auf ein breites Spektrum potenzieller Katastrophen und Betriebsrisiken aufrechtzuerhalten, die den Betrieb und die rechtzeitige Bereitstellung von Materialien und Services stören könnten. Criteo unterhält ein BCM-System, das regelmäßige Testintervalle vorsieht, um die Wirksamkeit der Kontrollen sicherzustellen. Auf ausdrückliche schriftliche Anfrage des Partners wird Criteo angemessene Abschätzungen und Fragen zur Wirksamkeit der Kontrollen seines BCM-Systems unterstützen.

Anwendungs- und Softwaresicherheit: Criteo unterhält angemessene Prozesse für die sichere Softwareentwicklung („SDL“), die sicherstellen, dass wirksame Freigabe-, Änderungs- und Konfigurationskontrollen durchgeführt und angemessene Anwendungssicherheitskontrollen beibehalten werden, um Unternehmens- und Kundendaten zu schützen. Dazu gehört auch, Softwareversionen und -komponenten auf angemessenem Niveau zu halten, um einen angemessenen Schutz zu gewährleisten.

Gerätesicherheit: Criteo sorgt für eine angemessene Gerätesicherheit für seine Mitarbeiter, die rund um die Uhr Sicherheitsüberwachung, Erkennung und Reaktion durch EDR-Endpunktschutz und angewandte Konfigurations-Baselines umfasst.

Netzwerksicherheit: Criteo unterhält angemessene Netzwerksicherheitskontrollen, um sich vor einer Unterbrechung der Serviceverfügbarkeit oder einem Sicherheitsverstoß zu schützen. Dazu gehören die Überwachung und Erkennung von Sicherheitsvorfällen rund um die Uhr und die Anwendung von Best Practices für die Sicherheit, einschließlich Segmentierung und Schwachstellen-Scans.

Verschlüsselung: Criteo verwendet geeignete Verschlüsselungscodes und -protokolle, um die Daten während der Übertragung zu schützen, und wendet eine geeignete Verschlüsselung oder gleichwertige Kontrollen an, wenn die Daten auf Wunsch über externe Medien übertragen werden müssen.

Meldung von Sicherheitsverletzungen: Criteo wird den Partner innerhalb von 72 Stunden über jede Verletzung der Sicherheit vertraulicher Daten (einschließlich personenbezogener Daten) informieren. Wenn ein Sicherheitsverstoß festgestellt wird, der sich auf vertrauliche Informationen auswirkt, wird Criteo auf eigene Kosten für Abhilfe sorgen, Untersuchungen durchführen und

in einem Bericht über einen Sicherheitsvorfall die entsprechenden Daten und Informationen zur Verfügung stellen, in dem die betroffenen Daten und die notwendigen damit zusammenhängenden Informationen aufgeführt sind.

Management von Sicherheitsvorfällen: Criteo wird rund um die Uhr Sicherheitserkennungs- und Reaktionskapazitäten vorhalten, um eine angemessene Erkennung und Reaktion auf tatsächliche und potenzielle Datensicherheitsrisiken für die Datenbestände von Criteo zu gewährleisten. Diese Kontrollen zum Management von Sicherheitsvorfällen werden von einem speziellen Sicherheitsteam durchgeführt und gewartet.

Schwachstellen-Management: Criteo unterhält und betreibt ein umfassendes Schwachstellen-Management-System mit angemessenen Kontrollen, die sich an den besten Praktiken und Standards der Branche orientieren. Zu diesen Kontrollen gehören Schwachstellen-Scans auf allen Plattformen der Produktionsumgebung, wobei die Berichterstattung, Analyse und Behebung der entdeckten Schwachstellen angemessen verwaltet wird. Solche Scans werden intern und extern durchgeführt.