ACCORD DE PROTECTION DES DONNÉES CRITEO

PRÉAMBULE

Le présent Accord de protection des données Criteo (ci-après l'« **APD** ») complète les Conditions générales de service de Criteo (les « **Conditions** ») ainsi que les Conditions spécifiques de service de Criteo (les « **CSS** ») ou tout autre accord applicable avec le Partenaire (collectivement, l'« **Accord** »), et est intégré par les présentes dans l'Accord conclu entre Criteo et le Partenaire pour la fourniture des Services Criteo.

Le présent Accord de protection des données décrit les obligations des Parties en matière de protection et de sécurité de tout traitement de Données à caractère personnel effectué dans le cadre de la fourniture des Services Criteo. Cela comprend le traitement des Données de Service si et uniquement dans la mesure où ces données contiennent des Données à caractère personnel, conformément aux exigences des Lois relatives à la protection des données.

Le présent Accord de protection des données est subdivisé selon les sections suivantes :

- **Section I : Conditions générales**
  - La Section I s'applique dès lors que le Partenaire a commandé des Services auprès de Criteo, quel que soit le type de Services commandés.

- **Section II : Conditions relatives aux responsables conjoints du traitement**
  - La Section II s'applique lorsque le Partenaire a commandé des Services pour lesquels Criteo et le Partenaire agissent en tant que Responsables conjoints du traitement, comme indiqué dans les Conditions de service spécifiques pertinentes (les « **Services de Responsables conjoints du traitement** »).

- **Section III : Conditions de Responsable du traitement à Sous-traitant (applicable exclusivement à Mabaya)**
  - La Section III s'applique lorsque le Partenaire a commandé des Services pour lesquels le Partenaire agit en tant que Responsable du traitement et Criteo agit comme que Sous-traitant, traitant les Données à caractère personnel pour le compte du Partenaire comme indiqué dans les Conditions de service spécifiques pertinentes (les « **Services de Responsable du traitement à Sous-traitant** »).

La Section I du présent APD s'applique toujours aux Parties. L'application des Sections II et/ou III dépendra du statut sous lequel Criteo opère et qui est spécifié dans les CSS ou dans tout autre arrangement applicable au Service commandé par le Partenaire.

Section I : Conditions communes

Les dispositions de la présente Section I « Conditions communes » s'appliquent toujours lorsque le Partenaire a commandé des Services à Criteo, quel que soit le type de Services commandés.

1 Définitions

Sauf indication contraire dans les présentes, les définitions figurant dans l'Accord s'appliquent au présent APD. Les définitions additionnelles énoncées ci-dessous s'appliqueront au APD.

« Autorité réglementaire »	désigne l'autorité publique ou l'agence gouvernementale responsable du contrôle du respect de la loi sur la protection des données, y compris, mais sans s'y limiter, la CNIL française (l'autorité de régulation supervisant Criteo.), le Bureau du commissaire à l'information du Royaume-Uni, l'Agence de protection de la vie privée de Californie ainsi que les procureurs généraux des États américains.
« Consentement »	désigne toute indication librement donnée, spécifique, informée et non ambiguë de la volonté de la Personne concernée par laquelle celle-ci, par une déclaration ou par une action affirmative claire, signifie son accord au Traitement des Données Personnelles la concernant.
« Données à caractère personnel »	désigne toute information identifiant, se rapportant, décrivant, pouvant être associée ou pouvant raisonnablement être liée à une personne physique ou un ménage identifié ou identifiable, traitée dans le cadre de la fourniture des Services Criteo concernés.

« Lois relatives à la protection des données »	désigne dans la mesure applicable toutes les lois et réglementations internationales, nationales, fédérales et régionales applicables en matière de protection des données et de la vie privée, y compris, mais sans s'y limiter : (a) le règlement général sur la protection des données (« EU GDPR »), (b) la loi britannique sur la protection des données (« UK GDPR »), (c) la loi californienne sur la protection de la vie privée des consommateurs (« CCPA ») et la loi californienne sur les droits à la vie privée (« CPRA »), (d) la loi de Virginie sur la protection des données des consommateurs (« VCDPA »), (e) la loi du Colorado sur la protection de la vie privée (« CPA »), (f) le Connecticut Data Privacy Act (« CTDPA »), (g) le Utah Consumer Privacy Act (« UCPA »), (h) le Oregon Consumer Privacy Act (« OCPA »), (i) le Texas Data Privacy and Security Act (« TDPSA »), (j) le Montana Consumer Data Privacy Act (« MTCDPA »), (k) le Korean Personal Information Protection Act (« PIPA ») ; telles qu'elles sont mises en œuvre dans chaque juridiction, ainsi que toute législation modificative ou de remplacement (ou similaire) de temps à autre. Par souci de clarté, la loi sur la protection des données comprend également toutes les exigences juridiquement contraignantes émises par les autorités compétentes en matière de protection des données i) encadrant le traitement et la sécurité des informations relatives aux personnes et prévoyant des règles pour la protection des droits et libertés de ces personnes en ce qui concerne le traitement des données les concernant, ii) spécifiant des règles pour la protection de la vie privée en ce qui concerne le traitement des données et les communications électroniques, ou iii) promulguant des droits pour les personnes qui sont opposables aux organisations en ce qui concerne le traitement de leurs données personnelles, y compris les droits d'accès, de rectification et d'effacement. Toute loi sur la protection des données citée dans le présent document ne s'applique au Partenaire que dans la mesure où les critères fixés par le droit applicable le prévoient.
« Personne concernée »	désigne une personne physique identifiable qui peut être identifiée, directement ou indirectement, en particulier par référence à un identifiant (par ex., un nom, un numéro d'identification, des données de localisation, un identifiant en ligne) ou à un ou plusieurs facteurs spécifiques à cette personne physique. Aux fins du présent APD, « Personne concernée » désigne les personnes physiques dont les Données à caractère personnel sont traitées dans le cadre de la fourniture des Services Criteo concernés.
« Responsable du traitement »	désigne la personne physique ou morale, l'autorité publique, l'agence ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du Traitement des Données à caractère personnel. En vertu de la Section II du présent APD, Criteo S.A., en tant que société mère du groupe Criteo, et le Partenaire agissent en tant que Responsables conjoints du traitement et, en vertu de la Section III du présent APD, le Partenaire agit en tant que Responsable du traitement. Le terme « Responsable du traitement » est considéré comme un « Business » en vertu du CPRA.
« Responsable du traitement conjoint »	désigne un Responsable du traitement agissant conjointement avec une ou plusieurs autres personnes. En vertu de la Section II du présent APD, Criteo et le Partenaire agissent en tant que responsables conjoints du traitement.
« RGPD »	Désigne la réglementation de l'UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la Directive 95/46/CE.
« Sous-traitant »	désigne une personne physique ou morale, une autorité publique, une agence ou un autre organisme qui traite les Données personnelles pour le compte du Contrôleur. En vertu de la Section II du présent APD, les sous-traitants qui peuvent être engagés par Criteo ou le Partenaire sont des Sous-traitants et, en vertu de la Section III du présent APD, Criteo agit en tant que Sous-traitant.
« Traitement »	désigne toute opération ou ensemble d'opérations effectuées sur des Données à caractère personnel ou sur des ensembles de Données à caractère personnel, par des moyens automatisés ou non, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la divulgation par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou la combinaison, la restriction, l'effacement ou la destruction.

« Violation de données à caractère personnel »	désigne une violation de la sécurité entraînant la destruction accidentelle ou illégale, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé aux Données à caractère personnel transmises, stockées ou autrement traitées.

Les termes « **Business** », « **Finalités commerciales** », « **Vente** », « **Prestataire de services** » et « **Action** » ont la même signification que dans la Loi sur la protection des données applicable, et les termes apparentés seront interprétés en conséquence.

2 Respect des Lois

2.1 Chaque Partie doit se conformer, et être en mesure de démontrer sa conformité à ses obligations respectives en vertu des Lois relatives à la protection des données et conformément au présent APD.

2.2 Le Partenaire reconnaît et convient spécifiquement que son utilisation des Services de Responsables conjoints du traitement et de Responsable du traitement à Sous-traitant est conforme aux Lois relatives à la protection des données.

3 Autorisations

3.1 Une Partie ne divulguera pas de Données à caractère personnel à l'autre Partie, sauf si la Partie divulgatrice garantit à l'autre Partie que cette divulgation est conforme aux Lois relatives à la protection des données et qu'elle s'est conformée à toute exigence applicable en matière d'information, de notification, d'autorisation ou de consentement de l'autorité publique compétente(s) ou des Personnes concernées, en ce qui concerne toute Donnée à caractère personnel fournie par la Partie divulgatrice à l'autre Partie. Chaque Partie divulgatrice doit conserver des preuves de son respect de ces exigences pendant la durée du Contrat et les fournir rapidement à l'autre Partie sur demande.

3.2 Rien dans le présent APD n'interdit ou ne limite les droits de Criteo à mettre en œuvre l'anonymisation des Données à caractère personnel traitées dans le cadre du Contrat, et dans la mesure requise par les Lois relatives à la protection des données, le Partenaire autorise par les présentes Criteo à mettre en œuvre des techniques d'anonymisation conformément aux Lois relatives à la protection des données. Par souci de clarté, les données résultant d'une anonymisation efficace et conforme ne sont pas soumises au présent APD et plus généralement aux Lois relatives à la protection des données.

4 Coopération

4.1 Les Parties coopéreront pour se conformer aux Lois relatives à la protection des données et pour remplir leurs obligations en vertu du présent APD.

4.2 Les Parties conserveront une documentation appropriée sur les activités de Traitement menées par chacune d'entre elles et sur leur conformité aux Lois relatives à la protection des données et au présent APD en ce qui concerne les Services de Responsables conjoints du traitement et de Responsable du traitement à Sous-traitant.

4.3 Dans le cas d'une enquête, d'une procédure, d'une demande formelle d'informations ou de documentation, ou de tout événement similaire en relation avec une autorité de protection des données et en relation avec les Services de Responsables conjoints du traitement ou de Responsable du traitement à Sous-traitant ou avec les Données à caractère personnel, les Parties traiteront rapidement et de manière adéquate les demandes de l'autre Partie concernant le Traitement des Données à caractère personnel en vertu du Contrat.

4.4 En cas de modification ou de nouvelle(s) loi(s) relative(s) sur la protection des données, les Parties s'engagent à apporter d'un commun accord toute modification ou révision raisonnablement nécessaire au présent DPA.

5 Délégués à la protection des données

5.1 Criteo et le Partenaire ont nommé un délégué à la protection des données. Le délégué à la protection des données de Criteo est joignable à l'adresse : dpo@criteo.com. Les coordonnées du délégué à la protection des données du Partenaire doivent être communiquées à Criteo.

Section II – Conditions relatives aux Responsables conjoints du traitement

6 Champ d'application de la présente section II

6.1 La présente Section II s'appliquera uniquement au Traitement des Données à caractère personnel effectué dans le cadre de la fourniture par Criteo des Services de Responsables conjoints du traitement commandés par le Partenaire.

6.2 Conformément à l'article 26 du RGPD, les Parties déterminent par les présentes leurs responsabilités respectives en matière de respect de leurs obligations en vertu du RGPD.

6.3 Aux fins du CPRA, le Partenaire est une « Business » et Criteo est un « Tiers ».

7 Obligations des Parties lorsqu'elles agissent en tant que Responsables conjoints du traitement

7.1 Lors du Traitement des Données à caractère personnel en tant que Responsables conjoints du traitement en vertu de la Section II du présent APD, chaque Partie convient de :

(a) Se conformer à toute exigence découlant des Lois relatives à la protection des données et ne pas exécuter ses obligations en vertu du présent APD et / ou demander à l'autre responsable conjoint d'exécuter ses obligations de manière à amener l'autre responsable conjoint à violer l'une de ses obligations en vertu des Lois sur la protection des données ;

(b) Prendre en compte tous les principes de protection des données prévus par les Lois relatives à la protection des données, y compris, à titre non limitatif, les principes de limitation des finalités, de minimisation des données, d'exactitude, de limitation du stockage, de sécurité, d'intégrité et de confidentialité, de transparence et de protection des Données à caractère personnel dès la conception et par défaut ;

(c) Tenir un registre du Traitement des Données à caractère personnel réalisé sous sa responsabilité ;

(d) Mettre en œuvre des mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité approprié aux risques présentés par le Traitement des Données à caractère personnel qu'il effectue (y compris pour ce qui concerne les Propriétés numériques du Partenaire), en particulier pour protéger les Données à caractère personnel contre la destruction accidentelle ou illégale ou la perte accidentelle, l'altération, la divulgation ou l'accès non autorisé ;

(e) Prendre toutes les mesures nécessaires pour remédier à toute Violation de données à caractère personnel relative aux Données à caractère personnel qu'il traite, atténuer ses effets, prévenir toute autre Violation de données à caractère personnel et, si nécessaire, informer l'autorité(s) compétente en matière de protection des données et les Personnes concernées ;

(f) Coopérer à la préparation des évaluations d'impact requises en matière de protection des données ;

(g) Effectuer toute évaluation, consultation et / ou notification aux autorités compétentes de protection des données ou aux Personnes concernées, en relation avec le Traitement qu'elles effectuent ; et

(h) Traiter toutes les demandes et / ou plaintes des Personnes concernées qu'elles reçoivent, en particulier les demandes relatives à l'exercice de leurs droits en vertu des Lois relatives à la protection des données, y compris les droits d'accès, de rectification, d'effacement et d'opposition et le droit de retirer le Consentement. Lorsqu'une Partie reçoit la demande de droit d'une Personne concernée concernant les Données à caractère personnel traitées par l'autre Partie, ladite Partie destinataire dirigera la Personne concernée vers la politique de confidentialité de l'autre Partie expliquant comment exercer sa demande de droit auprès de ladite autre Partie, afin de permettre à ladite autre Partie de répondre directement à la demande de la Personne concernée.

8 Obligations de Criteo

8.1 Criteo sera seule responsable, conformément aux Lois relatives à la protection des données et dans la mesure requise par celle-ci, de l'inclusion d'un lien vers la page de la Politique de confidentialité de Criteo (www.criteo.com/privacy) qui inclura des informations pour les Personnes concernées sur la manière de désactiver le Service Criteo (et d'insérer un lien de « désabonnement ») dans toutes les publicités diffusées sur les Propriétés numériques du Partenaire.

8.2 En tant que "third-party" au sens du CPRA: (a) l'utilisation des données personnelles par Criteo est limitée aux objectifs spécifiques identifiés dans l'Accord et Criteo ne dépassera pas ces objectifs spécifiques ; (b) Criteo respectera les obligations applicables et fournira le même niveau de protection de la vie privée que celui exigé d'un "Business" conformément au CPRA en ce qui concerne les données personnelles ; (c) Criteo accorde au Partenaire le droit, moyennant un préavis raisonnable, de prendre des mesures raisonnables et appropriées pour s'assurer que Criteo utilise les données personnelles d'une manière conforme au présent Accord et aux Lois relatives à la protection des données, y compris des mesures raisonnables et appropriées pour arrêter et remédier à l'utilisation non autorisée des données personnelles ; et (d) Criteo informera le Partenaire si elle détermine qu'elle ne peut plus respecter ses obligations en vertu des Lois relatives à la protection des données.

9 Obligations du Partenaire

9.1 Le Partenaire sera seul responsable, conformément à et dans la mesure requise par les Lois relatives à la protection des données de :

(a) Fournir aux Personnes concernées toutes les informations nécessaires en vertu des Lois relatives à la protection des données, y compris conformément aux Articles 13 et 14 du RGPD, concernant le Traitement des Données à caractère personnel en relation avec les Services de Responsables conjoints du traitement,

(b) Fournir un avis approprié sur les Propriétés numériques du Partenaire pour tout Traitement pertinent des Données à caractère personnel par Criteo pour les Services de Responsables conjoints du traitement, y compris en fournissant un lien vers la politique de confidentialité de Criteo (www.criteo.com/privacy),

(c) Recueillir et documenter les dispositions de Consentement ou de désabonnement, selon le cas, obtenues des Personnes concernées,

(d) Mettre en œuvre des mécanismes de choix pour demander un Consentement valide aux Personnes concernées ou des dispositions de désabonnement, selon le cas, conformément aux Lois relatives à la protection des données et, le cas échéant, aux exigences spécifiques des autorités de contrôle locales compétentes,

(e) Lorsque des dispositions de désabonnement sont applicables, offrir aux Personnes concernées le droit de refuser la vente et le partage de leurs Données à caractère personnel ou l'utilisation des Données à caractère personnel à des fins de publicité ciblée,

(f) Respecter les exigences applicables à la période de validité du Consentement recueilli et demander le Consentement aux Personnes concernées une fois cette période de validité expirée,

(g) Fournir rapidement à Criteo, sur demande et à tout moment, la preuve qu'un Consentement de la Personne concernée a été obtenu par le Partenaire.

Section III - Conditions de Responsable du traitement à Sous-traitant

10 Champ d'application de la présente section III

10.1 La présente Section III s'appliquera uniquement au Traitement des Données à caractère personnel effectué dans le cadre des Services de Responsable du traitement à Sous-traitant commandés par le Partenaire, agissant en tant que Responsable du traitement ou Business (selon le cas), pour lequel Criteo agit en tant que Sous-traitant ou Service Provider (selon le cas), et dont l'objet, la nature et la finalité, le type de Données à caractère personnel, les catégories de Personnes concernées et la durée du Traitement sont énoncés dans l'Annexe 1 « Services de Responsable du traitement à Sous-traitant - Détails du Traitement des Données à caractère personnel ».

11 Obligations du Partenaire

11.1 Le Partenaire ne fournira pas de Données à caractère personnel à Criteo, sauf si cela est nécessaire à l'exécution des Services Criteo et à moins que le Partenaire n'ait donné les avis nécessaires et obtenu les consentements nécessaires, dans chaque cas, de la part des Personnes concernées dont les Données à caractère personnel sont Traitées par Criteo en vertu de l'Accord. Le Partenaire devra, dans le cadre de son utilisation des Services Criteo, traiter les Données à caractère personnel conformément aux exigences de la Loi sur la protection des données et devra immédiatement

informer Criteo si le Partenaire enfreint une Loi sur la protection des données. Les instructions du Partenaire à Criteo relatives au Traitement des Données à caractère personnel doivent être conformes à la Loi sur la protection des données. Le Partenaire sera seul responsable de garantir l'exactitude, la légalité et la qualité des Données à caractère personnel et de s'assurer que le Traitement confié à Criteo dispose d'un fondement juridique adéquat conformément aux Lois sur la protection des données.

12 Obligations de Criteo

12.1 **Instructions du Partenaire.** Criteo traitera les Données à caractère personnel pour les Services de Responsable du traitement à Sous-traitant concernés uniquement selon les instructions documentées du Partenaire. Le Partenaire ne peut pas demander à Criteo de traiter les Données à caractère personnel d'une manière non compatible avec le Contrat et, plus particulièrement, avec le présent APD. Criteo informera immédiatement le Partenaire si Criteo estime raisonnablement ne pas être en mesure de suivre les instructions du Partenaire, ou si ces instructions ne sont pas compatibles avec les Conditions de service spécifiques ou plus généralement avec le Contrat.

12.2 **Données inexactes ou obsolètes.** Criteo informera le Partenaire si Criteo apprend que les Données à caractère personnel sont inexactes ou sont devenues obsolètes, et Criteo coopérera sur demande avec le Partenaire pour effacer ou rectifier lesdites données.

12.3 **Traitement des données à caractère personnel.** Dans la mesure où la Loi applicable en matière de protection des données l'exige, le Partenaire ne donnera instruction à Criteo de traiter les Données à caractère personnel qu'aux Finalités commerciales autorisées par la Loi applicable en matière de protection des données et ne divulguera les Données à caractère personnel à Criteo qu'aux fins limitées et spécifiées dans l'Accord. Le Partenaire se réserve le droit, après l'envoi d'un préavis raisonnable, de prendre des mesures raisonnables et appropriées pour s'assurer que Criteo utilise les Données à caractère personnel transférées d'une manière conforme aux obligations du Partenaire en vertu de la Loi applicable sur la protection des données, y compris des mesures raisonnables et appropriées pour arrêter et remédier à l'utilisation non autorisée des Données à caractère personnel.

Criteo ne doit pas : (a) vendre ou partager des Données à caractère personnel ; (b) conserver, utiliser ou divulguer des Données à caractère personnel à d'autres fins que les Finalités commerciales spécifiées dans l'Accord ; (c) conserver, utiliser ou divulguer des Données à caractère personnel en dehors de la relation commerciale directe entre le Partenaire et Criteo ; ou (d) combiner les Données à caractère personnel qu'il reçoit du Partenaire avec des Données à caractère personnel qu'il reçoit d'une ou de plusieurs autres personnes, ou pour le compte de celles-ci, ou qu'il collecte à partir de sa propre interaction avec les Personnes concernées, à condition que Criteo puisse combiner des Données à caractère personnel pour réaliser une Finalité commerciale (à l'exception des « services de publicité et de marketing », au sens de la Loi applicable en matière de protection des données). Criteo se conformera aux obligations applicables et fournira le même niveau de protection de la vie privée que celui requis par la Loi applicable sur la protection des données, et aidera le Partenaire par le biais de mesures techniques et organisationnelles appropriées pour se conformer aux exigences de la Loi sur la protection des données, en tenant compte de la nature du traitement. Criteo informera le Partenaire s'il détermine qu'il ne peut plus respecter ses obligations en vertu de la Loi applicable sur la protection des données.

12.4 **Mesures techniques et organisationnelles.** Criteo mettra en œuvre des mesures techniques et organisationnelles appropriées pour assurer la sécurité des Données à caractère personnel, y compris la protection contre une Violation de données à caractère personnel. Dans le respect de ses obligations en vertu du présent paragraphe, Criteo mettra au moins en œuvre les mesures techniques et organisationnelles indiquées en Annexe 2 « Annexe sécurité". Le Partenaire confirme par les présentes à Criteo qu'il considère que les mesures techniques et organisationnelles de Criteo telles qu'indiquées en Annexe 2 « Annexe sécurité » fournissent un niveau de sécurité approprié. Criteo aidera également le Partenaire à se conformer à ses obligations en matière de sécurité du Traitement des Données à caractère personnel, notamment en vertu de l'article 32 du RGPD.

12.5 **« Violation de données à caractère personnel ».** En cas de Violation de Données à caractère personnel concernant les Données à caractère personnel traitées par Criteo, Criteo prendra les mesures appropriées pour remédier à la Violation, y compris des mesures pour atténuer ses effets indésirables. Criteo informera également le Partenaire sans retard injustifié après avoir pris connaissance de la violation et avoir prévu le temps nécessaire pour fournir des informations pertinentes, y compris, par exemple, une description de la nature de la violation (y compris, si possible, les catégories et le nombre approximatif de Personnes concernées et de dossiers de Données à caractère personnel concernés), ses conséquences probables et les mesures prises ou proposées pour remédier à la violation, y compris, le cas échéant, les

mesures visant à atténuer ses effets indésirables possibles. En cas de Violation de Données à caractère personnel relative aux Données à caractère personnel traitées par Criteo, le Partenaire sera seul responsable de la notification aux Personnes concernées et/ou aux Autorités réglementaires, comme l'exige la Loi sur la protection des données, et Criteo coopérera avec le Partenaire et l'aidera à se conformer à toute demande d'une autorité compétente et/ou des Personnes concernées affectées, en tenant compte de la nature du Traitement et des informations à la disposition de Criteo. Avant de procéder à une telle notification, le Partenaire consultera Criteo et lui donnera la possibilité de faire des commentaires sur toute notification faite en lien avec une Violation de Données à caractère personnel. Aucune disposition du présent APD ne doit être interprétée comme obligeant Criteo à violer ou à retarder le respect de toute obligation légale qu'elle pourrait avoir en ce qui concerne une Violation de Données à caractère personnel. Criteo n'est pas responsable des obligations de gestion et de notification de la Violation de Données à caractère personnel décrites dans la présente section, à moins que la Violation de Données à caractère personnel ne soit causée par un manquement de Criteo aux obligations de sécurité prévues à la section 12.4 du présent APD ou par une autre violation, de sa part, de la Loi sur la protection des données.

12.6 **Accès aux Données à caractère personnel.** Criteo accordera l'accès aux Données à caractère personnel aux membres de son personnel uniquement dans la mesure de ce qui est strictement nécessaire à la mise en œuvre, à la gestion et au suivi du Contrat et conformément au présent APD. Elle veillera à ce que les personnes autorisées à traiter les Données à caractère personnel se soient engagées à un ou plusieurs accords de confidentialité ou soient soumises à une obligation légale de confidentialité appropriée.

13 **Droits des Personnes concernées.** Dans la mesure permise par la loi, Criteo informera rapidement le Partenaire de toute demande qu'elle a reçue d'une Personne concernée pour exercer les droits de la Personne concernée, y compris les droits de connaissances/accès, correction, suppression, restriction, objection, portabilité des données, désabonnement du Traitement et/ou de la Vente ou du Partage de Données à caractère personnel, limitation de l'utilisation ou de la divulgation de Données à caractère personnel sensibles, ou toute autre demande concernant les Données à caractère personnel de la Personne concernée, comme indiqué dans la Loi applicable sur la protection des données. Criteo ne répondra pas elle-même à la demande. Criteo aidera raisonnablement le Partenaire en mettant en œuvre des mesures techniques et organisationnelles appropriées, dans la mesure du possible, pour remplir ses obligations de réponse aux demandes des Personnes concernées d'exercer leurs droits en vertu de la Loi sur la protection des données, en tenant compte de la nature du Traitement. Dans la mesure permise par la loi, le Partenaire sera responsable de tous les coûts découlant de la fourniture d'une telle assistance par Criteo. Aucune disposition de la présente section 13 n'oblige Criteo à divulguer ou à révéler des secrets commerciaux.

13.1 **Évaluation d'impact sur la protection des données.** À la demande du Partenaire, à ses frais, et dans la mesure requise par la Loi sur la protection des données, Criteo aidera le Partenaire à se conformer à toute évaluation d'impact sur la protection des données à la demande du Partenaire, en tenant compte des informations à la disposition de Criteo. Dans la mesure requise par le RGPD ou le RGPD Royaume-Uni, Criteo fournira une assistance raisonnable au Partenaire dans le cadre de sa coopération ou de sa consultation préalable avec une Autorité réglementaire dans l'exécution de ses tâches relatives à la présente section 13.1.

13.2 **Sous-traitants secondaires.** Criteo peut engager des sous-traitants secondaires comme indiqué en Annexe 1 « Services de responsable du traitement à sous-traitant - Détails du traitement des données à caractère personnel **».** Le Partenaire donne à Criteo une autorisation générale pour engager d'autres Sous-traitants ultérieurs afin d'effectuer le Traitement pour les Services de Responsable du traitement à Sous-traitant concernés. Sur demande écrite du Partenaire, Criteo informera le Partenaire de tout changement concernant l'ajout ou le remplacement de Sous-traitants ultérieurs. Si le Partenaire s'oppose à ces modifications pour des motifs raisonnables [concernant la protection des données] dans les trente (30) jours suivant la notification par Criteo au Partenaire, les Parties discuteront de bonne foi en vue de trouver une solution mutuellement acceptable. Si les Parties ne parviennent pas à un accord, Criteo pourra résilier le Contrat en tout ou en partie en ce qui concerne uniquement les Services de Responsable du traitement à Sous-traitant concernés. Lors de l'engagement d'un autre Sous-traitant, Criteo conclura un accord contraignant pour ledit Sous-traitant et énoncera les mêmes obligations de protection des données ou des obligations plus strictes que celles énoncées dans le présent APD, en fournissant en particulier des garanties suffisantes pour mettre en œuvre des mesures techniques et organisationnelles similaires.

13.3 **Traitement des Données à caractère personnel en dehors des Instructions du Partenaire.** Nonobstant ce qui précède, si la loi applicable ou une décision contraignante d'une autorité compétente exige que Criteo traite des Données à

caractère personnel en dehors des instructions du Partenaire aux fins de fournir les Services de Responsable du traitement au Sous-traitant, Criteo en informera le Partenaire, sauf si la loi applicable l'interdit autrement.

13.4 **Audit.** Le Partenaire peut demander par écrit, à des intervalles raisonnables, que Criteo mette à la disposition du Partenaire des informations concernant la conformité de Criteo à ses obligations en vertu de la Section III du présent APD sous la forme d'une copie des audits ou certifications tiers les plus récents de Criteo.

Le Partenaire peut demander un audit sur site des activités de Traitement de Criteo décrites à la Section III du présent APD en fournissant à Criteo un préavis raisonnable. Un tel audit sur site ne peut être effectué que lorsque (i) les informations mises à disposition par Criteo comme indiqué ci-dessus sont insuffisantes, (ii) une violation des Données à caractère personnel s'est produite ou (iii) un tel audit est requis par les Lois relatives à la protection des données ou une autorité réglementaire.

Les Parties conviendront de l'étendue, du calendrier et de la durée de l'audit. L'audit ne doit pas interférer de manière déraisonnable avec les activités de Criteo.

Le Partenaire ne peut nommer qu'un auditeur tiers qui n'est pas un concurrent de Criteo. Ledit auditeur tiers conclura un accord de non-divulgation avec Criteo et le Partenaire avant de procéder à l'audit.

Après l'audit sur site, le Partenaire partagera rapidement les résultats de cet audit avec Criteo.

Les Parties mettront à la disposition d'une autorité réglementaire, sur demande, les informations visées à la présente clause, y compris les résultats de tout audit.

Le Partenaire supportera tous les coûts liés aux audits.

13.5 **Transfert de données à caractère personnel.** Tout transfert de données vers un pays tiers ou une organisation internationale par Criteo se fera uniquement sur la base d'instructions documentées du Partenaire conformément au Chapitre V du RGPD. Le Partenaire convient que, lorsque Criteo engage un sous-traitant ultérieur conformément à la Clause 13.2 pour mener des activités de Traitement spécifiques (au nom du Partenaire) et que ces activités de Traitement impliquent un transfert de Données à caractère personnel au sens du Chapitre V du RGPD, Criteo et le sous-traitant ultérieur peuvent assurer la conformité au Chapitre V du RGPD en utilisant les clauses contractuelles types adoptées par la Commission européenne conformément à l'Article 46(2) du RGPD, à condition que les conditions d'utilisation de ces clauses contractuelles types soient remplies.

13.6 **Conséquences de la résiliation.** Si le Partenaire résilie un Service de Responsable du traitement à Sous-traitant, ou si le Contrat expire ou prend fin pour quelque raison que ce soit, Criteo devra, au choix du Partenaire, supprimer toutes les Données à caractère personnel traitées uniquement pour ce Service de Responsable du traitement à Sous-traitant, ou restituer toutes ces Données à caractère personnel au Partenaire. Criteo certifiera, le cas échéant, que des copies desdites Données à caractère personnel ont été effacées, sur demande par écrit du Partenaire, sous toutes réserves de toute sauvegarde opérationnelle effectuée par Criteo pendant une période raisonnable conformément aux normes du secteur. Dans le cas où la loi applicable interdirait à Criteo d'effacer les Données à caractère personnel, Criteo garantit qu'elle continuera à assurer la conformité au présent APD et ne traitera ces Données à caractère personnel que dans la mesure et aussi longtemps que la loi applicable l'exige.

Les signataires autorisés des Parties ont dûment signé le présent APD :

PARTENAIRE	**CRITEO**
Signature: _____	Signature: _____
Nom: _____	Nom: _____
Fonction: _____	Fonction: _____
Date: _____	Date: _____

ANNEXE 1: Services de responsable du traitement à sous-traitant - Détails du traitement des données à caractère personnel (applicable exclusivement à Mabaya)

Catégorie de personnes concernées			
Catégories de Personnes concernées dont les Données à caractère personnel sont traitées	Utilisateurs des Propriétés numériques du Partenaires (« shoppers »)	Salariés du Responsable du traitement	Vendeurs (salariés / représentants)
Catégories de Données à caractère personnel traitées	Identifiants constitués d'une série de caractères (identifiant contenu dans un cookie ou autre) fournis par le Responsable du traitement (lorsque ces données sont qualifiées de Données à caractère personnel en vertu des Lois relatives à la protection des données)	Nom et adresses e-mail des salariés / représentants autorisés du Responsable du traitement	Adresses e-mail des Vendeurs (pour leur envoyer des rapports et des notifications)
Données à caractère sensible	N/A		
Nature du Traitement	Collecte, hébergement, traitement pour fournir le Service, effacement		
Finalité(s) pour lesquelles les Données à caractère personnel sont traitées pour le compte du Responsable du traitement	Faire correspondre les conversions aux clics (dans le contexte des Publicités)	Vérifications d'identité (page de connexion) Administration des comptes	Notification par e-mail aux Vendeurs
Durée du Traitement	Durée du Contrat		

Le Partenaire reconnaît et autorise l'utilisation par Criteo des entités suivantes en tant que sous-traitants ultérieurs, le cas échéant, en ce qui concerne les Services de Responsable du traitement à Sous-traitant concernés :

Sous-traitants secondaires .	**Objet du Traitement**	**Nature du Traitement**	**Catégories de personnes concernées**	**Catégories de Données à caractère personnel traitées**	**Durée du Traitement**
Amazon Web	Hébergement (centre de	Hébergement	Voir ci-dessus	Voir ci-dessus	Durée du Contrat

Services (AWS)	données en Irlande)				
Sendgrid	Envoi d'e-mails aux clients (États-Unis)	Utilisation des coordonnées pour envoyer des e-mails	Salariés du Partenaire	Adresses e-mail	Durée du contrat

Annexe 2 - Programme de sécurité de Criteo

La présente annexe relative à la sécurité (l'« **Annexe** ») présente les contrôles de sécurité relatifs au(x) Service(s) Criteo et à la gouvernance globale de la sécurité.

La présente Annexe complète les conditions entre Criteo et le Partenaire et fait partie de l'Accord. En cas de contradiction entre l'Accord et la présente Annexe, la présente Annexe prévaut.

1. **Définitions**

Les définitions suivantes appuient les dispositions spécifiées dans la présente Annexe :

Informations confidentielles : désigne, spécifiquement dans le contexte de la présente Annexe, les informations du Partenaire et de Criteo traitées, stockées et transmises par les plateformes de services Criteo et les actifs de données connexes, ainsi que les contrôles de sécurité associés appliqués pour protéger la sécurité des données.

Actifs de données : désigne toute plateforme technologique, tout composant, toute donnée ou toute information traitée par le biais des plateformes de produits des services Criteo traitant, transmettant ou stockant des Informations confidentielles.

Violation de données : désigne une violation de la sécurité entraînant la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès, accidentels ou illégaux, de Données à caractère personnel transmises, stockées ou autrement traitées.

Violation de la sécurité : désigne l'accès, l'utilisation, la divulgation, l'altération ou la destruction, réels ou potentiels, non autorisés des Informations confidentielles, ou un acte ou une omission qui compromet les données relatives aux services contractuels liés à la protection de la sécurité, de la confidentialité ou de l'intégrité des Informations confidentielles.

2. **Contrôles de sécurité**

Les contrôles de sécurité et de confidentialité suivants sont maintenus et pris en charge par Criteo en ce qui concerne les services Criteo :

Gouvernance et gestion de la sécurité : Criteo maintiendra un Système de gestion de la sécurité similaire à la norme ISO 27002, incluant d'autres bonnes pratiques en matière de confidentialité et de sécurité connues dans le secteur et des contrôles de sécurité complémentaires. Cela inclut une documentation appropriée (politiques de sécurité, processus, directives, normes, normes de configuration et contrôles de sécurité associés pour assurer une protection adéquate des actifs de données Criteo et du Partenaire tout au long du cycle de vie du Service.

Évaluations de la sécurité : Pas plus d'une fois par année civile et uniquement sur réception d'une demande écrite avec un préavis d'au moins trente (30) jours ouvrables, le Partenaire sera autorisé à effectuer des évaluations de sécurité sur le Système de gestion de la sécurité de Criteo et les contrôles de sécurité associés directement liés aux services fournis en tant que Sous-traitant. Les évaluations de la sécurité seront limitées à des questionnaires de sécurité détaillés, des requêtes ou des questions spécifiques liées aux services contractuels et excluent les audits physiques, les tests de pénétration, les scans ou d'autres activités intrusives. Les Évaluations de la sécurité doivent être effectuées de préférence par un auditeur tiers, qui sera soumis à la confidentialité et soumettra son rapport pour validation à Criteo avant que les résultats finaux ne soient fournis au Partenaire. Ces demandes seront rapidement prises en charge en donnant accès aux contrôles de sécurité de Criteo appliqués pour protéger les actifs de données de Criteo et du Partenaire contre les menaces, les risques et les vulnérabilités en matière de sécurité, les réponses étant fournies dans des délais raisonnables et présentées avec précision.

Assurance de la sécurité des tiers : Criteo maintiendra des contrôles d'assurance de sécurité appropriés pour gérer de manière adéquate les risques liés à la sécurité des données pour les services tiers afin de garantir la protection des actifs de données de Criteo et du Partenaire.

Formation en matière de sécurité : Criteo maintiendra des programmes appropriés de sensibilisation à la sécurité et à la confidentialité afin de protéger de manière proactive les actifs de données de Criteo et du Partenaire, avec un contenu aligné sur les meilleures pratiques du secteur pour atténuer les risques liés à la sécurité des données.

Contrôles de sécurité physique et environnementale : Criteo maintiendra des contrôles de sécurité physiques et environnementaux appropriés pour se protéger contre les risques liés à la sécurité des données et contre les risques en matière de confidentialité, d'intégrité et de disponibilité. Tous ces contrôles seront alignés sur les meilleures pratiques du secteur, des opérations et de sécurité applicables en matière de protection contre les risques liés à la sécurité physique et environnementale, notamment les contrôles d'accès physique, la surveillance de la sécurité physique et les protections environnementales contre les coupures de courant, les risques d'incendie et les risques opérationnels connexes.

Contrôle d'accès : Criteo maintiendra un système complet de gestion du contrôle d'accès conforme aux meilleures pratiques du secteur afin de protéger les actifs de données de Criteo et des clients avec une gouvernance appropriée pour l'accès, en assurant des contrôles appropriés pour l'autorisation et l'authentification, sur la base du principe du moindre privilège. Ces contrôles doivent inclure l'identification des comptes à privilèges avec une authentification multifactorielle (AMF) appropriée appliquée aux autorisations d'accès aux Informations confidentielles sur la sécurité. Les journaux d'accès de tous les comptes autorisés, généraux ou administratifs, seront collectés, surveillés et les autorisations seront examinées régulièrement.

Système de gestion de la continuité des activités (BCM) : Criteo maintiendra un Système de gestion de la continuité des activités (Business Continuity Management, « BCM ») qui détaillera les contrôles de continuité, les rôles, les responsabilités et les mesures de récupération afin de maintenir les exigences de disponibilité des Services contractuelles en réponse à un large éventail de catastrophes et de risques opérationnels potentiels qui pourraient perturber les opérations et la livraison en temps opportun des matériaux et des services. Criteo maintiendra un Système BCM qui prévoit des intervalles de test réguliers pour garantir l'efficacité des contrôles. Sur demande écrite spécifique du Partenaire, Criteo prendra en charge les évaluations et les questions raisonnables relatives à l'efficacité de ses contrôles de son Système BCM.

Sécurité des applications et des logiciels : Criteo maintiendra des processus appropriés de développement de logiciels sécurisés (Secure Software Development, « SDL ») qui garantissent que des contrôles efficaces des versions, des modifications et des configurations sont effectués et que des contrôles appropriés de la sécurité des applications sont maintenus pour protéger les actifs de données de l'entreprise et des clients. Il s'agit notamment de maintenir des versions logicielles et des composants à des niveaux appropriés pour assurer une protection adéquate.

Sécurité de l'appareil : Criteo maintiendra une sécurité appropriée des appareils pour ses salariés, qui comprend une surveillance, une détection et une réponse de sécurité 24 heures sur 24, 7 jours sur 7, 365 jours par an, grâce à la protection des terminaux EDR et à l'application de bases de configuration.

Sécurité du réseau : Criteo maintiendra des contrôles appropriés de sécurité du réseau pour se protéger contre toute interruption de la disponibilité du Service ou contre toute Violation de la sécurité. Il s'agira notamment de surveiller et de détecter les incidents de sécurité 24 heures sur 24, 7 jours sur 7, 365 jours par an, ainsi que d'appliquer les meilleures pratiques en matière de sécurité, notamment la segmentation et l'analyse des vulnérabilités.

Chiffrement : Criteo maintiendra des chiffrements et des protocoles appropriés pour protéger les données en transit, avec un chiffrement approprié ou des contrôles équivalents appliqués si les actifs de données doivent être transférés par le biais de supports externes, sur demande.

Signalement des violations de sécurité : Criteo informera le Partenaire de toute Violation de la sécurité des Informations confidentielles (y compris les Informations personnelles), dans les 72 heures. Si une faille de sécurité est détectée et a un impact sur des Informations confidentielles, Criteo, à ses propres frais, atténuera, enquêtera et fournira des données et informations

pertinentes appropriées dans un rapport d'incident de sécurité, détaillant les données affectées et les informations connexes nécessaires.

Gestion des incidents de sécurité : Criteo maintiendra des capacités de détection et de réponse en matière de sécurité, 24 heures sur 24, 7 jours sur 7, 365 jours par an, afin de garantir une détection et une réponse appropriées aux risques réels et potentiels pour la sécurité des actifs de données de Criteo. Ces contrôles de gestion des incidents de sécurité seront exploités et maintenus par une équipe de sécurité dédiée.

Gestion des vulnérabilités : Criteo maintiendra et exploitera un système complet de gestion des vulnérabilités, avec des contrôles appropriés alignés sur les meilleures pratiques et normes du secteur. Ces contrôles comprennent des analyses de vulnérabilité sur les plateformes de l'environnement de production, avec une gestion appropriée des rapports, des analyses et des mesures d'atténuation des vulnérabilités détectées. Ces analyses seront appliquées en interne et en externe.