

ACCORD SUR LA PROTECTION DES DONNÉES

dans le cadre de l'utilisation

d'une plateforme de marketing d'affiliation mise à disposition par Webgains

entre

L'Annonceur

et

WEBGAINS FRANCE SARL

(« **WBG** »)

(ci-après individuellement « la **partie** » et ensemble « les **parties** »)

EXPOSÉ PRÉALABLE

- (A) WBG exploite une plateforme de marketing d'affiliation permettant aux annonceurs de mettre à disposition des moyens publicitaires destinés à la distribution de leurs produits / services par les Publishers. Pour la participation à ce programme de marketing d'affiliation de WBG, il est nécessaire d'affecter ces moyens publicitaires d'un code de suivi fourni aux annonceurs par WBG. Ce n'est qu'ainsi que la fourniture des prestations par WBG aux annonceurs peut être techniquement mise en œuvre.
- (B) Parmi les Publishers enregistrés, les annonceurs peuvent choisir ceux dont ils souhaitent qu'ils se chargent de la diffusion des moyens publicitaires dans leurs circuits de distribution. La plateforme de marketing d'affiliation mise à disposition par WBG permet de recenser et d'analyser les ventes générées par les Publishers pour les annonceurs. Par ailleurs, WBG assure le reporting aux annonceurs et indique les rémunérations à verser aux Publishers pour la génération des ventes et à WBG pour l'utilisation de la plateforme.
- (C) WBG est contractuellement liée aussi bien au Publisher qu'à l'annonceur. La fourniture des services par WBG nécessite la communication de données à caractère personnel à WBG et le traitement de ces données pour que WBG puisse respecter ses obligations juridiques. Ces opérations comprennent notamment la facturation de la rémunération due aux Publishers au titre de leur rôle d'intermédiaire, la facturation de la rémunération due par l'annonceur au titre de l'utilisation de la plateforme et la refacturation de la rémunération des Publishers. Par ailleurs, la communication de données à WBG est nécessaire au développement des services et fonctions ainsi qu'à la prévention des abus et à la lutte contre la fraude.
- (D) Les **Parties A et B** du présent accord définissent les détails de ce traitement des données. La **Partie C** contient le modèle de l'accord des responsables conjoints du traitement qui s'applique entre l'annonceur et le Publisher en cas d'utilisation par le Publisher du moyen publicitaire mis à disposition par l'annonceur. En mettant à disposition son moyen publicitaire sur la plateforme de marketing d'affiliation, l'annonceur propose la conclusion de l'accord des responsables conjoints du traitement (conformément à la Partie C) que le Publisher accepte de conclure s'il sélectionne le moyen publicitaire.
- (E) Le présent accord est destiné à garantir une protection adéquate des données à caractère personnel dans le cadre de leur communication et traitement conformément à la législation applicable en la matière. Par ailleurs, les parties souhaitent mettre en œuvre des mesures appropriées au regard de la protection de la vie privée ainsi que des droits et libertés fondamentaux.

Ceci étant exposé, les parties conviennent de ce qui suit :

1. DÉFINITIONS

1.1 Dans le présent accord, les termes ci-dessous ont la signification suivante :

- (a) Les termes « **données à caractère personnel** », « **responsable du traitement** », « **sous-traitant** », « **traitement** », « **personne concernée** », « **sous-traitant ultérieur** », « **mesures techniques et organisationnelles** » et « **autorité de contrôle** » ont la signification qui leur est donnée dans le RGPD.
- (b) Un « **Pays à niveau de protection adéquat** » est un pays qui ne fait pas partie de l'Espace économique européen et pour lequel la Commission européenne a décidé qu'en tenant compte de la législation interne ou des engagements internationaux souscrits, il assure un niveau de protection adéquat des données à caractère personnel.

- (c) Par « **Conditions générales de vente** » ou « **CGV** », on entend les *Conditions Générales de Vente* communiquées à l'Annonceur par WBG, y compris tous les accords, conditions et autres mandats régissant l'utilisation de la plateforme.
- (d) L'« **Accord** » désigne le présent accord sur la protection des données.
- (e) Les « **Conventions** » désignent l'Accord de sous-traitance et l'Accord des responsables conjoints du traitement (voir ci-dessous).
- (f) Par « **Accord de sous-traitance** » ou « **AST** », on entend les dispositions de la **Partie A**.
- (g) « **WBG** » désigne la société Webgains France SARL, 21, Boulevard Haussmann, 75002 Paris, France (ci-après « WBG » ou « le prestataire »).
- (h) Par « **Accord des responsables conjoints du traitement** », on entend les dispositions des **Parties B et C**. Cet accord définit le transfert et le traitement de données à caractère personnel entre WBG et l'Annonceur (**Partie B**) ainsi que l'interaction entre l'Annonceur et le Publisher / les Publishers dans la mesure où elle concerne la protection des données conformément à l'article 26 du RGPD (**Partie C**). Ces dispositions s'appliquent, que les parties doivent ou non être considérées comme des responsables conjoints du traitement selon l'article 26 du RGPD. Quelle que soit la réponse à cette question, elles doivent garantir une protection adéquate du transfert et du traitement des données à caractère personnel.
- (i) La « **Sous-traitance** » désigne le traitement de données à caractère personnel pour le compte du responsable du traitement au sens de l'article 28 du RGPD. L'Annonceur agit en tant que responsable du traitement, WBG agit en tant que sous-traitant.
- (j) L'« **Annonceur** » désigne toute entreprise qui utilise les Services de marketing d'affiliation de WBG sur la base des CGV ou de tout accord contractuel similaire.
- (l) Le « **Publisher** » désigne toute personne physique ou morale qui s'est inscrite sur la plateforme de WBG sur la base des CGV et qui assure sur ses sites / dans ses circuits de distribution la promotion des moyens publicitaires fournis par un Annonceur.
- (m) Le « **RGPD** » désigne le règlement (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 (Règlement général sur la protection des données).
- (n) Par « **Responsable(s) conjoints du traitement** », on entend plusieurs responsables (conjoints) du traitement de données à caractère personnel qui déterminent conjointement les finalités et les moyens de ce traitement (cf. article 26 du RGPD).
- (o) Un « **Etat membre** » désigne un Etat membre de l'Union européenne ou un Etat faisant partie de l'Espace économique européen.
- (p) Les « **Services de marketing d'affiliation** » comprennent les prestations décrites dans les CGV ou auxquelles celles-ci font référence, y compris la mise à disposition par WBG de la plateforme de marketing d'affiliation qui permet aux Annonceurs de gérer les processus de ce marketing. Ces services incluent l'enregistrement des ventes générées par les Publishers et le reporting correspondant.

- 1.2 Il est précisé que, dans le cadre du présent Accord :
- (a) le renvoi à des dispositions légales inclut tous les textes subséquents adoptés sur la même base ;
 - (b) le renvoi au présent Accord inclut l'ensemble de ses Parties (actuellement A, B et C) et leurs annexes ;
 - (c) les titres ne doivent pas être pris en compte pour l'interprétation de l'Accord ;
 - (d) en cas de conflit ou de contradiction entre les clauses du présent Accord, le conflit ou l'incohérence sera résolu par la clause qui prime.

2. CHAMP D'APPLICATION

- 2.1 L'Accord de sous-traitance (Partie A) et l'Accord des responsables conjoints du traitement (Partie B) s'appliquent entre les parties dans leurs rôles de responsable du traitement ou de sous-traitant des données à caractère personnel transférées et traitées conformément aux dispositions de la Partie A ou B. Les Parties A et B précisent les processus et la responsabilité incombant à chaque partie dans le cadre de ces processus au titre des différents traitements des données.
- 2.2 En fonction du processus mis en œuvre, chaque partie peut agir en tant que responsable du traitement, de responsable conjoint du traitement ou de sous-traitant, étant précisé que, dans le cadre des processus initialement définis par le présent Accord, seule WBG agit également en tant que sous-traitant au sens de l'article 28 du RGPD et l'Annonceur en tant que mandant.
- 2.3 En cas de mandat donné à un Publisher par l'intermédiaire de la plateforme de marketing d'affiliation de WBG, l'Annonceur conclura un accord de responsabilité conjointe avec le Publisher / les Publishers concerné(s), conformément à l'article 26 du RGPD (Partie C : Accord des responsables conjoints du traitement). WBG se charge d'imposer aux Publishers enregistrés sur sa plateforme de marketing d'affiliation l'obligation de conclure l'Accord des responsables conjoints du traitement (Partie C) s'ils acceptent un mandat. Les parties considèrent que la conclusion de l'Accord des responsables conjoints du traitement (Partie C) ne donne pas naissance à un lien contractuel civil entre l'Annonceur et le Publisher. Elles conviennent qu'en ce qui concerne l'utilisation de Services de marketing d'affiliation, l'Annonceur (et le Publisher) ne feront valoir leurs droits que dans le cadre de leurs liens contractuels avec WBG.
- 2.4 En agissant en tant que sous-traitant ou de responsable du traitement, chaque partie s'engage à imposer à tout sous-traitant ultérieur éventuellement recruté le respect d'un niveau de protection au moins comparable à celui prévu par les Conventions en veillant à ce que le sous-traitant ultérieur respecte des exigences adéquates en matière de sécurité et de protection des données, avant qu'un accord soit mis en œuvre avec lui.
- 2.5 Afin de garantir un niveau de protection adéquat dans le cadre du transfert et du traitement de données à caractère personnel, il est précisé que les principes définis dans la Partie B s'appliquent à tout traitement et transfert de données entre les responsables du traitement.

3. RESPECT DES DISPOSITIONS CONTRACTUELLES

- 3.1 Les parties s'engagent à respecter les obligations qui leur incombent dans le cadre du présent Accord dans leur rôle de responsable du traitement et/ou de sous-traitant.
- 3.2 Chaque partie peut exercer à l'égard de l'autre les droits résultant du présent Accord dans les limites dans lesquelles l'autre partie agit envers elle dans le rôle correspondant.

4. MODIFICATIONS

- 4.1 Les parties conviennent que le présent Accord peut être modifié et/ou complété conformément à la procédure décrite ci-après.
- 4.2 WBG peut modifier ou compléter le présent Accord si elle estime que cela est nécessaire, notamment pour que les parties respectent les dispositions applicables en matière de protection des données.
- 4.3 Si elle envisage la mise en application de modifications ou de compléments, WBG préviendra l'autre partie au moins six (6) semaines avant l'entrée en vigueur prévue en lui envoyant un texte écrit (par exemple, un courriel). Si, dans les quatre (4) semaines qui suivent la réception de cette information, l'autre partie n'a pas communiqué son refus par l'envoi d'un texte écrit et qu'elle continue à utiliser les Services de marketing d'affiliation après la fin de ce délai, les modifications et/ou compléments seront réputés acceptés. Dès la fin du délai de six (6) semaines fixé ci-dessus, l'Accord s'appliquera alors dans sa version modifiée.
- 4.4 Dans son message, WBG rappellera à l'autre partie les conséquences qu'entraîne la poursuite de l'utilisation des Services de marketing d'affiliation sans contestation de sa part.
- 4.5 Si l'autre partie s'oppose à l'application des modifications ou compléments, les parties entameront des discussions constructives pour régler d'un commun accord leurs divergences et les contestations. Si elles ne parviennent pas à trouver une solution, aussi bien WBG que l'Annonceur pourra résilier le présent Accord ou les mandats concernés en respectant un préavis de quatre (4) semaines.

5. DURÉE ET CESSATION

- 5.1 Le présent Accord entre en vigueur au moment de la confirmation de son application par l'Annonceur selon la procédure préalablement indiquée, étant précisé que la date d'entrée en vigueur est celle à laquelle la dernière partie donne son consentement par la signature du présent Accord ou de toute autre manière (notamment en acceptant ces conditions par voie électronique, par courriel ou par consentement tacite si elle utilise les Services de marketing d'affiliation sans s'opposer à l'Accord). Dès l'entrée en vigueur, chaque partie est liée par les dispositions prévues par le présent Accord.
- 5.2 Le présent Accord est conclu pour une durée indéterminée. Il prend automatiquement fin au moment de la cessation du contrat basé sur les CGV et l'utilisation des Services de marketing d'affiliation.

6. RÉSILIATION

- 6.1 Toute résiliation prononcée dans le cadre du présent Accord (« **résiliation** ») doit être notifiée par écrit.
- 6.2 Si, en application des CGV, WBG a le droit de résilier le contrat basé sur les CGV et l'utilisation des Services de marketing d'affiliation, elle peut également résilier le présent Accord.
- 6.3 Chaque partie conserve son droit de résilier le présent Accord à titre extraordinaire.

7. CESSION

L'Annonceur ne peut céder ou transférer des droits ou obligations résultant du présent Accord s'il n'a pas préalablement obtenu l'accord écrit de WBG.

8. INVALIDITE PARTIELLE

- 8.1 Si tout ou partie d'une disposition du présent Accord est invalide, nulle ou inapplicable, la légalité, la validité et l'applicabilité de toutes les autres dispositions ne sera pas mise en cause.
- 8.2 Les parties s'engagent à remplacer la disposition nulle par une disposition valable dont l'effet se rapproche le plus possible du but économique visé par la disposition nulle. Cette clause s'applique mutatis mutandis s'il s'avère que l'Accord présente des lacunes.

9. LOI APPLICABLE

Le lieu d'exécution est Paris, France. En cas de litige, les tribunaux de Paris sont compétents. Le présent Accord est régi par la loi de la République Française, à l'exclusion des règles de conflit. La Convention des Nations-Unies du 11/04/1980 sur les contrats de vente internationale de marchandises ne s'applique pas.

10. APPLICATION PAR RAPPORT AUX CGV

- 10.1 Dans toutes les circonstances pour lesquelles le présent Accord ne prévoit pas de dispositions, y compris la responsabilité des parties dans le cadre de la fourniture ou de l'utilisation des Services de marketing d'affiliation, les clauses des CGV sont applicables.
- 10.2 En cas de contradiction entre les dispositions de l'Accord et celles des CGV, les dispositions de l'Accord sont prépondérantes.

Partie A

Accord de sous-traitance

Préambule

Le présent Accord de sous-traitance (« **Convention constituant la Partie A** ») concrétise les obligations incombant aux parties en matière de protection des données dans le cadre de la sous-traitance définie ci-dessous. Les dispositions de la présente Partie A concernent le traitement de données à caractère personnel par WBG pour le compte de l'Annonceur ou par des tiers mandatés par le mandataire (ci-après « les sous-traitants ultérieurs »).

1. Rôles des participants et responsabilités

Pour pouvoir mettre en œuvre les Services de marketing d'affiliation, l'Annonceur en tant que mandant est tributaire du traitement de données à caractère personnel par WBG en tant que mandataire. A cet effet, le mandataire réalise pour le mandant des prestations dans les limites définies en **annexe 1** de la présente Partie A.

2. Objet du mandat, nature, finalités et limites du traitement des données

- 2.1 Le mandat a pour objet les activités de traitement définies ci-après et/ou dans les CGV, y compris les documents qui les concrétisent ou un accord complémentaire ou une commande (ci-après ensemble « le **mandat** »), telles qu'elles sont réalisées par WBG pour le compte et selon les instructions données par l'Annonceur.
- 2.2 Le type et les catégories des données à caractère personnel collectées et/ou traitées ainsi que les catégories des personnes concernées par la gestion des données à caractère personnel dans le cadre de ce mandat sont définis en **annexe 1**.
- 2.3 Les finalités, la nature et la portée de la collecte, du traitement et/ou de l'utilisation des données à caractère personnel dans le cadre du mandat sont définies en **annexe 1** de la présente Partie A.

3. Responsabilité et droits du responsable du traitement de donner des instructions

- 3.1 En ce qui concerne le traitement des données à caractère personnel réalisé par le mandataire dans le cadre du mandat, seul le mandant est responsable de l'appréciation de sa légalité au regard de la législation applicable en matière de protection des données.
- 3.2 Le mandataire ne traite les données à caractère personnel du mandant que pour exécuter les obligations de l'Accord de sous-traitance ou du contrat principal ou les instructions individuelles complémentaires visées à l'alinéa 2.
- 3.3 Dans le cadre du mandat, le mandant se réserve le droit le plus étendu de donner des instructions concernant la nature et les finalités du traitement des données, le type de données à caractère personnel et les catégories de personnes concernées. Il peut concrétiser l'exercice de ce droit en donnant des instructions individuelles. Le droit du mandant de donner des instructions pour le traitement des données à caractère personnel est concrétisé de façon exhaustive par les fonctions fournies dans le cadre des applications et des systèmes.
- 3.3 L'application des dispositions de l'article 3.2 est restreinte dans la mesure où cette restriction s'impose au mandataire en vertu du droit de l'Union européenne ou du droit des Etats membres auquel il est soumis. Dans ce cas, le mandataire informera le mandant de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

- 3.4 Si le mandataire estime qu'une instruction constitue une violation de dispositions applicables en matière de protection des données, il en informera le mandant immédiatement. Le mandataire pourra suspendre l'exécution de cette instruction jusqu'à ce qu'elle soit confirmée ou modifiée par le mandant.

4. Instructions et personne autorisées à donner des instructions

- 4.1 Le mandant ou la personne dûment mandatée par lui donnera toutes ses instructions par l'envoi d'un texte (par courrier, fax ou courriel). Si une instruction est exceptionnellement donnée oralement, le mandant enverra sans délai une confirmation par fax ou par courriel.
- 4.2 Toute instruction ou information à donner à l'autre partie en application du présent Accord sera adressée aux personnes désignées en annexe 2.

5. Obligations du mandataire

- 5.1 Le mandataire n'est pas autorisé à rectifier ou effacer des données à caractère personnel ou à limiter leur traitement, sauf si une instruction lui a été donnée en ce sens ou si l'effacement est effectué en application de l'article 15 du présent contrat (cessation du contrat). Toute demande d'une personne concernée exerçant son droit de rectification, à l'effacement ou au verrouillage de ses données doit être transmise au mandant sans délai.
- 5.2 Le traitement des données n'aura lieu qu'au sein de l'Union européenne ou dans un autre Etat ayant adhéré à l'Accord sur l'Espace économique européen. Tout transfert vers un pays tiers nécessite l'autorisation préalable du mandant. Si celui-ci autorise une dérogation, un niveau de protection adéquat doit être garanti conformément aux articles 44 et suivants du RGPD.
- 5.3 Les données ou les informations pouvant en être déduites ne seront ni conservées ni copiées sur les terminaux ou supports de données du mandataire, sauf si ces opérations sont indispensables à l'exécution du mandat.
- 5.4 Les informations dont le mandant peut avoir besoin pour tenir un registre complet des activités de traitement lui seront fournies par le mandataire sur simple demande.
- 5.5 Le mandataire s'engage à mettre en place une structure interne destinée à assurer la conformité à la loi et à utiliser cette structure notamment pour exécuter les dispositions et obligations prévues en matière de protection des données par l'Accord de sous-traitance. Cela inclut également - si nécessaire - une aide à la réalisation d'une analyse d'impact sur la protection des données.
- 5.6 Le mandataire a désigné un délégué à la protection des données dans la mesure où cette désignation lui est imposée par la loi. Le nom et les coordonnées de ce délégué dûment qualifié figurent en **annexe 2**. En cas de changement de ces informations, le mandataire informera le mandant sans délai.

6. Confidentialité du traitement des données et obligation du personnel de respecter les instructions

- 6.1 Le mandataire s'engage à prendre les mesures nécessaires pour que le personnel ayant accès aux données à caractère personnel dans le cadre de l'exécution du mandat ne traite ces données que conformément aux instructions données par le responsable du traitement, sauf si le prestataire est tenu de traiter ces données objet du contrat conformément au droit de l'Union européenne ou au droit des Etats membres.
- 6.2 En choisissant et en déployant son personnel, le mandataire veillera à ce que celui-ci respecte la législation en matière de protection des données et qu'il s'interdise de transmettre à des tiers les informations provenant du mandant ou de les utiliser de toute autre manière.
- 6.3 Le mandataire imposera à toutes les personnes agissant sous son autorité et ayant accès aux données à caractère personnel, objet du contrat, dans le cadre de l'exécution du mandat l'obligation de traiter ces données conformément au contrat.
- 6.4 Le mandataire n'affectera à ses tâches que des employés préalablement formés au respect de la législation en matière de protection des données. Il garantit que tous les employés chargés du traitement

des données transférées dans le cadre du présent contrat s'engagent à respecter la confidentialité ou sont soumis à une obligation de confidentialité appropriée prévue par la loi.

7. Procédure en cas de demandes de personnes concernées ou de tiers

- 7.1 S'il reçoit une demande ou une injonction émanant d'une autorité de contrôle de la protection des données ou d'un journaliste concernant l'objet du présent contrat, le mandataire informera le mandant par courriel dans les 48 heures qui suivent la réception, étant précisé que les jours de travail sont ceux qui sont travaillés en France.
- 7.2 En tant que responsable du traitement, le mandant est responsable du respect des droits des personnes concernées. Sauf instructions contraires expressément données, seul le mandant est chargé de répondre aux demandes des personnes concernées. Si le traitement de demandes de personnes concernées nécessite le concours du mandataire, notamment en cas d'exercice du droit d'accès, de rectification, à la limitation du traitement, à la portabilité ou à l'effacement des données, le mandataire prendra les mesures nécessaires conformément aux instructions données par le mandant.
- 7.3 Si une telle demande lui est adressée par une personne concernée, le mandataire informera sans délai (dans les 48 heures) la personne autorisée à donner des instructions pour le mandant en lui communiquant toutes les informations nécessaires. Les parties définiront éventuellement la procédure à suivre pour l'échange d'informations en cas de demandes de personnes concernées.

8. Sous-traitants ultérieurs

- 8.1 Si le mandataire souhaite faire appel à des sous-traitants ultérieurs dans le cadre de l'exécution du mandat, il doit obtenir l'autorisation du mandant. Avant de faire appel à un sous-traitant ultérieur et de lui communiquer des données à caractère personnel provenant du mandant, le mandataire préviendra celui-ci en lui envoyant un texte écrit. Le mandant est réputé avoir donné son autorisation s'il ne s'est pas opposé au recrutement du sous-traitant dans les six semaines qui suivent la notification.
- 8.2 Pour que le mandant puisse donner son autorisation au recrutement d'un sous-traitant ultérieur, le mandataire lui indiquera le nom et les coordonnées de celui-ci en précisant l'objet, la nature, la portée et les finalités du traitement des données concrètement prévu. Le mandataire vérifiera lui-même le respect des mesures de sécurité informatique par le sous-traitant ultérieur conformément aux dispositions de l'annexe 4. Si le mandant le demande, il lui communiquera les constatations faites à cette occasion. Le mandant ne refusera d'autoriser le recrutement du sous-traitant ultérieur que pour un motif légitime.
- 8.3 Un sous-traitant ultérieur ou un sous-traitant ultérieur de second rang établi dans un pays tiers (ne faisant pas partie de l'Union européenne / de l'Espace économique européen) ne peut être engagé que si les exigences du RGPD sont respectées.
- 8.4 Si le recours à la sous-traitance est autorisé, le mandataire sélectionnera soigneusement le sous-traitant ultérieur pour que l'exécution des obligations contractuelles soit assurée. Il rédigera le contrat à conclure avec le sous-traitant ultérieur de façon à ce que les dispositions relatives à la protection des données correspondent à celles de l'Accord de sous-traitance. Il veillera notamment à ce que le contrat garantisse au mandant l'exercice de ses droits de disposer et d'effectuer des contrôles, tels qu'ils sont prévus par le présent Accord. Ces dispositions contractuelles doivent notamment prévoir que le mandant peut directement exercer son droit de contrôle auprès du sous-traitant ultérieur, sans préjudice de la responsabilité du mandataire quant à l'intervention du sous-traitant ultérieur. Le mandataire renseignera le mandant à sa demande sans délai sur les dispositions du contrat ayant une importance pour l'exercice du contrôle ainsi que sur l'exécution par le sous-traitant ultérieur des obligations portant sur la protection des données.
- 8.5 Les sous-traitants ultérieurs d'ores et déjà admis figurent en **annexe 3**, étant précisé que l'autorisation est donnée sous réserve qu'avant le début du traitement des données, le mandataire documente le respect des mesures de sécurité des données et que les dispositions du présent article 8 soient respectées. Une liste actualisée des sous-traitants peut toujours être consultée sur <https://www.webgains.com/public/en/privacy-sub-processors/>.

- 8.6 Le mandataire vérifiera régulièrement (au moins une fois par an) le respect de ces obligations par le sous-traitant ultérieur en procédant à des contrôles appropriés. En cas de manquement aux obligations, il veillera à ce qu'il y soit remédié. Les contrôles et les mesures prises en cas de constatation de carences seront dûment documentés. Les rapports seront fournis au mandant à sa demande.
- 8.7 Aucune autorisation n'est exigée pour les contrats de sous-traitance portant sur des services qui ne nécessitent pas la conclusion d'un accord de sous-traitance, notamment les services accessoires, tels que les services postaux d'acheminement du courrier et des colis, les services de télécommunication ou de nettoyage, les prestations de personnes soumises au secret professionnel (conseillers fiscaux, avocats, médecins externes à l'entreprise, auditeurs comptables).

9. Définition des mesures techniques et organisationnelles

- 9.1 La sélection du mandataire sera notamment basée sur sa conclusion que le sous-traitant ultérieur présente des garanties suffisantes quant à la mise en œuvre des mesures techniques et organisationnelles en matière de sécurité des données et que le traitement des données à caractère personnel répond aux exigences de la loi et garantit un niveau de sécurité du traitement approprié au regard du risque pour les droits et libertés des personnes physiques concernées par le traitement.
- 9.2 Sauf s'il s'agit d'un cas de télémaintenance / d'accès à distance, le mandataire veillera à ce que les objectifs de protection visés à l'article 32, paragraphe 1 du RGPD, tels que la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services utilisés pour le traitement des données ainsi que leur résilience au regard de la nature, de la portée, du contexte et des finalités du traitement puissent être atteints. Par ailleurs, il garantit qu'en cas d'incident physique ou technique, la disponibilité des données et l'accès à celles-ci seront rapidement rétablis et que le chiffrement le plus large sera utilisé pour le transport et la conservation des données.
- 9.3 En vue d'assurer le traitement des données à caractère personnel conformément au mandat, le mandataire a évalué les risques en appliquant une méthodologie reconnue tenant compte du degré de probabilité et de la gravité des risques pour les droits et les libertés des personnes concernées.
- 9.4 Dans le domaine relevant de sa responsabilité, le mandataire garantit la mise en œuvre de mesures techniques et organisationnelles appropriées et conformes à l'état des connaissances afin que les dispositions relatives à la protection des données soient respectées et que le risque lié au traitement des données soit durablement atténué. Le concept de protection des données décrit en annexe 4 présente en détail les mesures techniques et organisationnelles choisies en fonction du risque déterminé en tenant compte des objectifs de protection et de l'état des connaissances, notamment des systèmes informatiques du mandataire et des processus de traitement mis en œuvre par celui-ci. Ce concept est défini de façon contraignante par les parties.
- 9.5 Le traitement des données objet du contrat est autorisé en télétravail à condition que le mandataire garantisse la prise de mesures de sécurité appropriées au caractère critique du traitement des données. Ces mesures doivent être comparables à celles qui sont prises pour le traitement des données au bureau. Le mandataire s'engage à prendre les précautions techniques et organisationnelles nécessaires à cet effet et à en justifier sur demande.
- 9.6 Les mesures techniques et organisationnelles étant soumises au progrès technique et au développement, le mandataire est autorisé à mettre en œuvre des mesures alternatives adéquates, à condition que leur niveau de sécurité ne soit pas inférieur à celui des mesures définies. Toute modification importante touchant à la sécurité des données (par exemple, une modification de l'organisation du traitement des données assuré en sous-traitance) doit être préalablement convenue avec le mandant. Le mandataire s'engage à tester, à analyser et à évaluer l'efficacité des mesures techniques et organisationnelles destinées à assurer la sécurité du traitement (article 32, paragraphe 1, point d) du RGPD) dès lors qu'une raison particulière le justifie et au moins une fois par an. Il communiquera au mandant les conclusions et l'intégralité du rapport d'audit.
- 9.7 Le mandataire communiquera au mandant son concept de protection et de sécurité des données ainsi que son concept de gouvernance de la sécurité informatique de la sous-traitance si le mandant le lui demande.

10. Obligations générales de contrôle et d'information du mandataire

- 10.1 Si le mandataire estime qu'une instruction constitue une violation de dispositions applicables en matière de protection des données, il en informera le mandant immédiatement en lui envoyant un texte écrit. Le mandataire peut suspendre l'exécution de cette instruction jusqu'à ce qu'elle soit confirmée ou modifiée par le mandant. Le mandataire n'est pas autorisé à vérifier le respect des dispositions du droit matériel.
- 10.2 Le mandataire vérifiera régulièrement et au moins une fois par année civile le respect des exigences du présent Accord qui le concernent, notamment celles définies en **annexe 4** pour la sécurité des données. La vérification et les conclusions seront dûment documentées.
- 10.3 Si le mandataire estime qu'une instruction donnée par le mandant en matière de sécurité des données est insuffisante, il informera le mandant immédiatement.

11. Violations à notifier par le mandataire / perte de données

- 11.1 Le mandataire informera le mandant immédiatement si des dysfonctionnements apparaissent ou si la législation en matière de protection des données, des dispositions contractuelles, des exigences résultant du présent Accord de sous-traitance ou des instructions du mandant n'ont pas été respectées par lui ou son personnel ou s'il suspecte une violation des dispositions visées ci-dessus ou des irrégularités dans le cadre du traitement des données à caractère personnel. Il adressera cette information par fax ou par courriel aux personnes autorisées à donner des instructions pour le mandant, telles qu'elles sont désignées en annexe 2.
- 11.2 En ce qui concerne l'obligation de notification incombant au mandant à l'égard de l'autorité de contrôle de la protection des données et/ou des personnes concernées, le mandataire informera le mandant immédiatement (dans les 24 heures) de tout incident ne permettant pas d'exclure l'hypothèse que des données ont échappé au contrôle ou que des tiers ont pu y accéder ou risquent d'y accéder. Dans ce cas, le mandant peut exiger que le mandataire prête son concours à l'élucidation immédiate des faits, au traitement de l'incident et à la prise de mesures destinées à remédier à la violation des données à caractère personnel ou à en atténuer les conséquences.
- 11.3 Si le mandataire constate qu'un non-respect de la sécurité informatique ou une violation de données à caractère personnel qu'il traite pour le compte du mandant a entraîné une destruction ou une divulgation non autorisée, une perte ou une altération de données ou tout autre accès non autorisé à celles-ci (« incident de sécurité informatique ») ou s'il dispose d'éléments justifiant cette hypothèse, il en informera immédiatement le mandant en lui communiquant par un texte écrit toutes les informations sur la date et l'heure de survenance, la nature et l'étendue de cet incident / ces incidents. Cette information doit exposer la nature de la prise de connaissance des données par une personne non autorisée et, à titre complémentaire, les conséquences potentiellement préjudiciables de cet incident de sécurité informatique.
- 11.4 Le mandataire tiendra un registre de tous les incidents de sécurité informatique ayant affecté le traitement des données prévu par le présent contrat. Sur demande, il communiquera ce registre au mandant.

12. Contrôle par le mandant

- 12.1 Le mandant ou une personne dûment mandatée par lui est autorisé à contrôler le respect par le mandataire de toutes les instructions et dispositions du présent contrat et des exigences en matière de protection des données dans la mesure où elles s'appliquent au traitement des données objet du contrat. Ces contrôles, y compris les audits réguliers, seront effectués aux heures d'ouverture habituelles sans donner lieu à aucune facturation. Le mandataire s'engage à tolérer de tels contrôles et à assister le mandant conformément aux dispositions de l'alinéa (3) ci-dessous.
- 12.2 Le mandataire confirmera le respect des mesures de sécurité décrites en annexe 4 en présentant une attestation établie par une personne indépendante (délégué à la sécurité informatique, délégué à la

protection des données, auditeur informatique) conformément au modèle joint en **annexe 5**. La remise de cette attestation ne limite en rien le droit de contrôle prévu par l'alinéa 1 ci-dessus.

- 12.3 Sur demande, le mandataire communiquera au mandant toutes les informations nécessaires à la justification du respect de toutes les obligations résultant de l'Accord de sous-traitance et des dispositions applicables en matière de protection des données, y compris l'obligation de rendre compte. Le mandataire accorde au mandant tous les droits d'accès, d'information et de consultation nécessaires à la réalisation des contrôles. Il s'engage notamment à permettre au mandant d'accéder aux installations informatiques et aux documents présentant un rapport avec la collecte et l'utilisation de données communiquées par le mandant pour que celui-ci puisse effectuer ces contrôles et audits. En réalisant les contrôles, le mandant tiendra raisonnablement compte de l'exercice de l'activité par le mandataire et de ses intérêts de confidentialité légitimes.
- 12.4 La réalisation du contrôle et ses conclusions seront consignés dans un procès-verbal.
- 12.5 Conformément aux dispositions applicables en matière de protection des données, le mandant et le mandataire sont soumis aux contrôles publics par l'autorité de contrôle compétente. A la demande du mandant, le mandataire fera ses meilleurs efforts pour assister le mandant dans le cadre de procédures administratives de contrôle si et dans la mesure où celles-ci portent sur le traitement de données du mandant qui fait l'objet du présent contrat.

13. Exécution des mandats / cessation du contrat

13.1 Sauf dispositions contraires, les dispositions suivantes sont applicables :

(a) En cas d'exécution de mandats individuels, le mandataire effacera irrémédiablement dans les trois (3) mois qui suivent l'exécution du mandat toutes les données à caractère personnel fournies par le mandant.

(b) Si la durée de l'Accord de sous-traitance correspond à celle du contrat principal ou d'une convention de fourniture de prestations et qu'il ne s'agit pas d'un mandat individuel, les données fournies dans le cadre de l'exécution du contrat ne seront effacées que sur instruction du mandant.

(c) En lieu et place de la suppression, le mandant peut exiger le renvoi des données.

- 13.2 Dès la fin de l'exécution d'un mandat individuel, le mandataire certifiera au mandant spontanément qu'il a entièrement détruit ou irrémédiablement supprimé les données fournies, les données éventuellement conservées temporairement ainsi que tous les outils d'essai et le matériel à mettre au rebut. La suppression / destruction sera documentée de façon appropriée, par exemple, par l'établissement d'un procès-verbal. Sur demande, cette documentation sera fournie au mandant.
- 13.3 Le mandataire conservera au-delà de la fin du contrat toute documentation permettant de justifier de la régularité du traitement des données en respectant les délais de conservation prévus par la loi. A la fin du contrat, il peut remettre cette documentation au mandant pour se décharger de cette obligation.
- 13.4 Le mandant ou une personne dûment habilitée par lui peut vérifier si les données ont été entièrement renvoyées ou supprimées conformément au contrat et si les outils d'essai et le matériel à mettre au rebut ont été dûment détruits par le mandataire. Ce contrôle peut être effectué sur place par une inspection de l'équipement informatique utilisé dans les locaux du mandataire. Le mandant annoncera ce contrôle un respectant un préavis raisonnable.
- 13.5 Si la durée du présent contrat dépend de celle du contrat principal et qu'il est mis fin à ce dernier, le mandataire ne pourra continuer à conserver et à traiter les données au-delà de la fin du contrat principal que dans la mesure où cela est nécessaire à la bonne mise en œuvre de la cessation du présent contrat.

14. Annexes

Les annexes suivantes font partie intégrante du présent Accord :

- Annexe 1 : Instructions pour le traitement des données pour le compte du mandant

- Annexe 2 : Personnes à contacter
- Annexe 3 : Sous-traitants agréés préalablement
- Annexe 4 : Exigences en matière de sécurité des données
- Annexe 5 : Attestation du respect de la sécurité des données

PARTIE A

Annexe 1 : Instructions à WBG pour le traitement des données pour le compte de l'Annonceur

La présente annexe indique les instructions concrètes à respecter pour le traitement des données à caractère personnel dans le cadre de la fourniture des prestations.

Description du mandat	
Base des instructions	<p>Sur la base de la description des prestations convenues entre l'Annonceur et WBG, le responsable du traitement donne l'instruction au sous-traitant d'effectuer le traitement des données conformément :</p> <ul style="list-style-type: none"><input checked="" type="checkbox"/> aux CGV accompagnées d'une description concrète des prestations et<input checked="" type="checkbox"/> à la concrétisation ci-dessous : 1
Objet / nature / portée / spécification du traitement	<ul style="list-style-type: none"><input checked="" type="checkbox"/> Services informatiques dont la nature est précisée ci-dessous pour :<ul style="list-style-type: none">• le placement de cookies sur les terminaux des utilisateurs si ceux-ci ont donné leur consentement sur le site de l'Annonceur,• le recensement de l'accès aux offres (moyens publicitaires) de l'Annonceur, tel qu'il est enregistré grâce au code de suivi fourni par WBG et intégré par l'Annonceur à ses moyens publicitaires,• le recensement des Publishers participant à une transaction.<hr/><input checked="" type="checkbox"/> Services publicitaires dont la nature est précisée ci-dessous pour :<ul style="list-style-type: none">• l'établissement et la fourniture d'analyses concernant les données conservées pour l'Annonceur en utilisant les outils d'analyse mis à disposition par WBG.<hr/><input checked="" type="checkbox"/> Prestations de services dont la nature est précisée ci-dessous pour :<ul style="list-style-type: none">• l'établissement de rapports sur la base des données générées pour l'Annonceur afin de renseigner les Publishers intervenant pour celui-ci,• le calcul de la rémunération des Publishers,• le calcul de la rémunération due au titre de l'intervention de WBG,• l'analyse des données générées afin de détecter toute tentative de fraude et autre utilisation abusive de la plateforme,• la télémaintenance et l'assistance en cas de problèmes techniques.<hr/><input checked="" type="checkbox"/> Communication de données à WBG en application de l'Accord des responsables conjoints du traitement (voir Partie 2).
Finalités du traitement par le mandataire des données à caractère personnel des personnes concernées	<p>Recensement des ventes générées par les Publishers (transactions) sur la plateforme mise à disposition par le mandataire et établissement d'analyses pour le mandant, y compris fourniture d'analyses concernant l'ampleur des activités de vente réalisées pour l'Annonceur. Par ailleurs, WBG recense pour l'Annonceur les Publishers ayant participé à la vente afin de lui permettre de rattacher la rémunération aux différents Publishers.</p>

	<p>Pour le recensement correct, WBG fournit un code de suivi repris par le mandant et intégré à ses moyens publicitaires diffusés par les Publishers. Ce service fourni par WBG en tant que prestataire du mandant inclut le placement de cookies sur le terminal de l'utilisateur si celui-ci a donné son consentement.</p>
Début et fin du traitement	<input checked="" type="checkbox"/> en continu <input type="checkbox"/> mandat individuel Début : _____ Fin : _____ (à durée indéterminée, le cas échéant)
Personnes concernées (catégories)	<input checked="" type="checkbox"/> Clients <input checked="" type="checkbox"/> Clients potentiels <input checked="" type="checkbox"/> Autres : données des Publishers
Types de données à caractère personnel	<input checked="" type="checkbox"/> Données des transactions : identifiant des transactions et des Publishers, références des commandes, horodatage <input checked="" type="checkbox"/> Données du contrat : informations sur le produit, pays de l'utilisateur, montant <input checked="" type="checkbox"/> Données de facturation : montant de la vente, monnaie, type de commission <input checked="" type="checkbox"/> Informations sur le terminal / navigateur de l'utilisateur, identifiant des cookies, de la référence cache <input checked="" type="checkbox"/> Autres : identifiant de la campagne, du programme, de l'étude probabiliste, de l'événement, de la référence
Mode de communication des données	<input type="checkbox"/> SFTP <input checked="" type="checkbox"/> HTTPS (lien de téléchargement) <input checked="" type="checkbox"/> intégration de l'application de WBG via le script de tracking
Délai de renvoi / de suppression au terme du mandat	<input checked="" type="checkbox"/> 3 mois <input checked="" type="checkbox"/> 6 semaines <input type="checkbox"/> _____

PARTIE A

Annexe 2 : Personnes autorisées à donner des instructions, délégué à la protection des données

1. Personnes autorisées à donner des instructions pour le mandant

Interlocuteurs du mandant :

- le signataire du contrat lui-même
- les mandataires sociaux ou fondés de pouvoir du mandant
- l'utilisateur principal du compte du programme

2. Destinataires des instructions chez le mandataire

Interlocuteurs du mandataire :

Fonctions :	Webgains CEO
actuellement exercées par:	
Nom :	Richard Dennys
E-mail :	Rdennys@webgains.com

Remplaçants :

Nom :	Vittorio Lorenzoni
E-mail :	Vlorenzoni@webgains.it

3. Délégué à la protection des données du mandataire

Nom :	Dr. Stefan Drewes
E-mail :	data-privacy@webgains.com, datenschutz@webgains.de
Téléphone :	+49 228 / 90 24 80 70

interne externe

PARTIE A**Annexe 3 : Sous-traitants agréés**

N°	Fournisseur / prestataire	Lieu d'implantation	Finalités
1	Webgains Ltd, Third Floor, 21 Farringdon Road, London, EC1M 3HA	Angleterre	Gestion de l'application informatique, assistance informatique
2	Amazon Web Services, Inc	Irlande et Angleterre	Service d'hébergement, assistance
3	Pulsant Ltd	Angleterre	Service d'hébergement
4	Toute autre société du groupe Webgains établie dans l'Union européenne et engagée en tant que sous-traitant ultérieur conformément à l'article 8 de la Partie A si la campagne est réalisée sur l'ensemble du territoire de l'Union européenne	Sites de WBG dans l'Union européenne (soit actuellement en France, Angleterre, Espagne et Italie)	Assistance dans le cadre de campagnes réalisées sur l'ensemble du territoire de l'Union européenne / gestion de la plateforme de WBG
5	Neory GmbH	Allemagne	Solutions de marquage de conteneurs informatiques
6	HPS Newco Ltd	Allemagne et Pays-de-Galles	Etablissement de statistiques et contrôle de la qualité
7	Device Atlas Ltd.	Irlande	Assistance technique dans le cadre du recensement des transactions
8	Marketing Town Ltd (ancienne société Tech Essence Ltd)	Belgique, Angleterre, Pays-Bas, Suisse	Prestataire de services de tracking

PARTIE A

Annexe 4 : Mesures de sécurité informatique

Pour le traitement concret des données, un niveau de sécurité adapté au risque pour les droits et libertés des personnes physiques concernées par le traitement est garanti. A cet effet, les objectifs de protection visés par l'article 32, alinéa 1 du RGPD, notamment la confidentialité, l'intégralité et la disponibilité des systèmes et services ainsi que leur résilience quant à la nature, la portée, le contexte et les finalités des traitements, sont pris en compte de manière à atténuer ce risque de façon constante par des mesures techniques et organisationnelles.

Dans son concept de sécurité informatique, le prestataire a défini les objectifs de sécurité, un processus de sécurité informatique et un système de gestion informatique afin de garantir la protection des données à caractère personnel par la prise de mesures techniques et organisationnelles appropriées. Sur la base des exigences résultant de ce concept de sécurité informatique, les risques liés au traitement des données, les conséquences potentielles pour les personnes concernées et le degré de probabilité de réalisation du risque ont été déterminés. Conformément à l'exposé du concept de sécurité informatique, les mesures techniques destinées à garantir la sécurité des données ont été définies en tenant compte de l'état des connaissances et des coûts de mise en œuvre.

La conformité aux exigences résultant des dispositions légales, telles qu'elles sont prévues par le RGPD, et les principes d'une comptabilité régulière (GoB), est assurée selon le concept de « gestion de la sécurité informatique » qui prévoit non seulement des définitions, fonctions, attributions et responsabilités claires, mais aussi les mesures techniques et organisationnelles définies dans la présente annexe conformément à l'article 32 du RGPD. La mise en œuvre de ces mesures est constamment et continuellement contrôlée et vérifiée.

Les mesures techniques et organisationnelles décrites ci-dessous (« MTO ») sont celles qui ont été choisies en fonction du risque déterminé pour garantir la sécurité des données en tenant compte des objectifs de protection et de l'état des connaissances conformément à l'article 32 du RGPD. Elles reposent sur la grille suivante établie pour définir le niveau de protection :

Niveau de protection	Données à caractère personnel	Exemples (s'il s'agit de données isolées ; en cas de cumul de données, un niveau de protection plus élevé peut être approprié !)	Gravité des dommages possibles
A	Données auxquelles la personne concernée a donné libre accès	Annuaire téléphonique, sites Internet librement accessibles, réseaux sociaux librement accessibles	faible
B	Données dont le traitement non conforme ne comporte, a priori, pas de risque d'atteinte particulière, mais auxquelles la personne concernée n'a pas donné libre accès	Fichiers publics dont l'accès est limité, consultation du livre foncier, réseaux sociaux non librement accessibles, IBAN masqué (noircissement des six derniers chiffres), données de base de clients, date et lieu de naissance	faible
C	Données dont le traitement non conforme risque de porter atteinte à la personne concernée au niveau de sa position sociale ou de sa situation économique (« réputation »)	Revenus, données fiscales, contraventions, données de passeports, IBAN (intégral), données de contrats, de livraisons, de commandes	calculable

D	Données dont le traitement non conforme risque de porter gravement atteinte à la personne concernée au niveau de sa position sociale ou de sa situation économique de la (« existence »)	Placement dans un établissement, délinquance, évaluations professionnelles, certificats de travail, données de santé, dettes, saisies, données relevant d'une catégorie particulière selon l'article 9 du RGPD	substantielle
E	Données dont le traitement non conforme risque de porter atteinte à la santé, à la vie ou à la liberté de la personne concernée	Données de personnes susceptibles d'être victimes d'une infraction, programmes de protection des témoins	considérable
F	Données traitées dans le cadre de la télémaintenance / de l'accès à distance	Dispositions particulières qui tiennent compte de la situation spécifique liée à la télémaintenance / à l'accès à distance	

Les parties ont constaté que le traitement de données à caractère personnel défini dans le cadre du présent Accord de sous-traitance nécessite la protection définie ci-dessus :

Niveau de protection	Cocher la case utile
A	<input type="checkbox"/>
B	<input type="checkbox"/>
C	<input checked="" type="checkbox"/>
D	<input type="checkbox"/>
E	<input type="checkbox"/>
F	<input type="checkbox"/>

La liste suivante présente les mesures techniques et organisationnelles convenues pour garantir le niveau de protection C dont les parties estiment qu'il est approprié aux besoins.

Si les parties ont constaté que, pour certains traitements des données, le besoin de protection est plus important, les mesures complémentaires prises pour garantir la réalisation des objectifs de protection sont documentées dans le descriptif de la procédure correspondante.

I. Mesures organisationnelles destinées à garantir la sécurité des données

Le prestataire maintient une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement des données. Cette procédure doit également garantir que les mesures prises pour assurer la sécurité des données correspondent à l'état des connaissances, ce dont le prestataire justifiera à toute demande du mandant.

II. Mesures techniques destinées à garantir la sécurité des données

Afin d'assurer la sécurité des données, le mandataire prendra les mesures suivantes dont il garantit le respect par des contrôles effectués dans le cadre des mesures organisationnelles :

Objectif de protection : la confidentialité

Il s'agit de faire en sorte qu'aucune personne non autorisée, qu'il s'agisse d'un employé ou d'un tiers, ne puisse prendre connaissances de données à caractère personnel. La réalisation de cet objectif de sécurité nécessite un contrôle de l'accès aux locaux, aux installations et aux données. Il faut empêcher tout accès non autorisé au matériel informatique. Par ailleurs, le présent chapitre définit les exigences à respecter pour la séparation des mandants afin de garantir le rattachement des données au responsable du traitement concerné.

1. Contrôle de l'accès aux locaux

Contrôle de l'accès aux locaux abritant les installations informatiques : ce contrôle doit empêcher toute personne non autorisée de s'approcher d'une installation informatique. Une telle installation comporte l'unité centrale, y compris les lecteurs intégrés, et tous les périphériques connectés, tels que terminaux, ordinateurs, imprimantes, traceurs, enregistreur-lecteur de bandes magnétiques, etc. Les terminaux utilisés pour un accès à distance font également partie de l'installation informatique.

A l'intérieur des bureaux, le contrôle de l'accès aux ordinateurs peut être assuré, à titre d'exemple, par des mesures empêchant les clients de s'approcher des ordinateurs ou de consulter les écrans.

Mesures nécessaires à la réalisation des objectifs de protection
Réglementation de l'accès aux locaux par des personnes extérieures à l'entreprise, par exemple par :
<ul style="list-style-type: none">la définition de dispositions applicables à l'accès par des personnes extérieures à l'entreprisel'enregistrement des entrées et sorties des personnes extérieures à l'entreprisela mise en place d'un accueil central (gardien / accueil)la délivrance de badges de visiteursl'autorisation de la présence de personnes extérieures à l'entreprise uniquement si un membre du personnel est présentla récupération des dispositifs d'accès à l'expiration de l'autorisation
Réglementation de l'accès aux locaux par des personnes faisant partie de l'entreprise, par exemple par :
<ul style="list-style-type: none">la désignation des personnes autorisées à accéder physiquement aux locaux concernés / espaces sécurisés et la définition de l'étendue de leur autorisationla délivrance de dispositifs d'accès (par exemple, cartes à puce, enregistrement)l'enregistrement des entrées et sorties des membres du personnel
Désignation des personnes autorisées à accéder aux locaux abritant les ordinateurs / serveurs
Mesures destinées à garantir que seules les personnes autorisées peuvent accéder aux locaux abritant les ordinateurs / serveurs
Mise en place d'armoires / de caissons mobiles pouvant être fermés à clé
Dispositions applicables à l'utilisation des clés si l'entreprise utilise des clés (fermeture des portes à clé, remise de clés uniquement aux personnes autorisées, utilisation et conservation d'une clé de fermeture centralisée)
Mesures destinées à sécuriser le site (sécurisation des cages d'escalier, gaines et fenêtres, surveillance du site)

Sécurisation de l'entrée (système de fermeture, lecteur de cartes)
Fenêtres anti-cambriolage

2. Contrôle de l'accès aux installations

L'utilisation d'installations informatiques par des personnes non autorisées (employés ou personnes extérieures à l'entreprise) doit être empêchée. Il s'agit d'identifier et d'authentifier les personnes qui accèdent aux installations. Ce contrôle a également pour but d'empêcher tout accès externe aux installations informatiques (par exemple, à partir d'une connexion à Internet : protection contre les pirates informatiques).

Exigences
Authentification des utilisateurs dans le système informatique, c'est-à-dire identification par le nom de l'utilisateur et le mot de passe ou par un système de double authentification
Dispositions applicables à l'attribution des mots de passe
Mots de passe personnels
Mots de passe comportant au moins dix caractères dont des caractères spéciaux, chiffres, lettres en minuscules et majuscules
Gestion des droits
Enregistrement des accès
Définition par l'utilisateur lui-même
Péremption à l'expiration du délai fixé
Blocage de l'accès après trois tentatives infructueuses
Interdiction de communication les mots de passe à des tiers
Dispositions applicables en cas d'absence (congés, maladie, etc.)
Verrouillage des cinq derniers mots de passe utilisés
Blocage immédiat de l'autorisation d'un salarié quittant l'entreprise
Contrôle régulier de la validité des autorisations (une fois par an)
Sécurisation des postes de travail équipés d'un écran dès que l'utilisateur s'absente sans arrêter le système (protection du mot de passe pendant l'affichage de l'écran de veille après 5 à 15 minutes en fonction du risque d'abus)
Cloisonnement des réseaux internes pour les protéger contre tout accès externe (pare-feu, chiffrement, VPN)

3. Contrôle de l'accès aux données

Ce contrôle vise à restreindre l'accès aux données par les employés et les tiers autorisés à ce qui est prévu par leur autorisation. Par ailleurs, dans le cadre de la gestion des données à caractère personnel, il faut empêcher toute lecture, copie, modification ou suppression (effacement) non autorisée. Ces mesures concernent aussi bien les données conservées dans les systèmes informatiques que celles qui se trouvent sur les supports lisibles par machine ou sur papier.

Exigences
Etablissement de profils d'utilisateurs, c'est-à-dire définition de l'autorisation d'accéder aux données à caractère personnel faisant l'objet du traitement
Distinction entre autorisation de lire, de modifier et d'effacer les données
Délivrance des autorisations aux employés et auxiliaires d'exécution selon le principe du strict minimum : l'accès aux applications et composants du système n'est autorisé que s'il est nécessaire au travail à effectuer
Etablissement et mise en œuvre d'un concept d'autorisations <ul style="list-style-type: none"> • mise en place de droits d'administrateurs
Gestion des droits d'accès par un administrateur du système
Cryptage de tous les appareils (téléphones portables, ordinateurs portables, etc.)
Cryptage du transfert des courriels

Ecrans de veille
Séparation entre fonctionnement à l'essai et fonctionnement en production
Configuration de l'équipement informatique de manière à désactiver tous les services et composants qui ne sont pas nécessaires à la réalisation de la prestation concernée. Vérification annuelle de cette configuration.
L'attribution des autorisations doit être dûment documentée et comporter une étape de validation.
Les supports de données à mettre au rebut doivent être éliminés de façon à assurer la non-divulgaration de données en utilisant des moyens conformes à l'état de la technique et à la norme applicable (DIN 66399:2012) ou en confiant cette tâche à une entreprise spécialisée qui détruit ces supports en garantissant un niveau de sécurité équivalent ou supérieur. Pendant leur stockage et transport, les supports de données à détruire doivent être protégés par des mesures appropriées contre tout accès non autorisé.
La maculature (tirages de listings, de lettres, etc. à détruire) doit être éliminée de façon à assurer la non-divulgaration de données en utilisant une déchiqueteuse d'un niveau de sécurité P_4 conformément à la norme DIN 66399:2012. A défaut, cette élimination doit être confiée à une entreprise spécialisée qui détruit les documents en garantissant un niveau de sécurité équivalent ou supérieur.
Interdiction pour les employés d'utiliser Internet au moment où ils ont accès aux données du mandant.
Interdiction pour les employés d'utiliser leur compte de messagerie électronique à des fins personnelles s'ils traitent des données du mandant.

4. Contrôle de la séparation

Selon le principe de la séparation, les données collectées à des finalités différentes doivent être traitées séparément (interdiction d'enchaînement). Il s'agit de garantir la limitation des finalités des données à caractère personnel par des mesures techniques et organisationnelles. L'obligation de séparation a une importance particulière dans le cadre de la sous-traitance si des données de plusieurs mandants sont conservées dans le même système. Si cette séparation ne peut être garantie par des mesures techniques, par exemple, un logiciel de contrôle d'accès, une conservation séparée est nécessaire.

Exigences
Concept d'autorisations définissant les droits d'accès
Base de données à architecture multi-tenant

Objectif de protection : l'intégrité

Il s'agit de garantir que les processus et systèmes informatiques respectent en permanence les spécifications définies afin de préserver la validité, l'intégralité et l'exactitude des données traitées. Les informations doivent être exactes et complètes, provenir de l'auteur et seules les personnes dûment autorisées doivent pouvoir les modifier. Pour atteindre cet objectif de protection, il est nécessaire de prendre des mesures visant à garantir l'intégrité des données lors de leur transfert. Par ailleurs, il faut pouvoir attribuer toute modification des données à la personne qui l'a effectivement effectuée (contrôle de la saisie).

5. Contrôle du transfert

Ce contrôle porte sur tout mode de transfert de données à caractère personnel, que ce soit à l'aide de supports de données ou de réseaux de communication. Le contrôle du transfert vise à empêcher toute utilisation non autorisée pendant le transfert des données (lecture, copie, modification ou suppression / effacement), étant précisé que par transfert, on entend aussi bien la transmission à des tiers que la communication dans le cadre de la sous-traitance entre le mandant et le mandataire et la personne concernée.

Exigences
Documentation indiquant le destinataire des données, les voies de transport / de transfert, les personnes autorisées à transférer les données et les données à transférer
Transfert authentifié et suffisamment crypté avant que les données soient transférées si la voie de transmission n'est pas sécurisée

6. Contrôle de la saisie

Le contrôle de la saisie vise à disposer d'une documentation permettant d'identifier la personne responsable de la saisie (non) autorisée ou erronée de données. Il doit être possible de consulter l'enregistrement des données à caractère personnel dans le système informatique qui comporte également les postes de travail non connectés au réseau, tels que les PC. La saisie à contrôler comporte aussi bien l'enregistrement initial des données que leur modification et effacement (suppression).

Exigences
Délivrance d'autorisations d'accès consultables (traçables données par écrit)
Journalisation des saisies, modifications et effacements de données à caractère personnel
Réglementation de l'autorisation d'accès aux données des journaux
Utilisation de sommes de contrôle

Objectif de protection : la disponibilité et la résilience

En cas d'incident physique ou technique, il doit être possible de rétablir rapidement la disponibilité des données à caractère personnel et l'accès à celles-ci. A cet effet, les données doivent être protégées contre toute perte et destruction accidentelle qui pourrait être provoquée par un dégât des eaux, la foudre, une coupure de courant, un incendie, un sabotage, un vol, etc. La résilience a pour but d'atteindre une certaine stabilité du système face au risque de défaillance ou d'attaque. Cette exigence ayant une importance particulière en cas d'externalisation de services (hébergement de données), le contrôle de l'exécution du mandat donné à cet effet est également précisé ci-après.

7. Contrôle de la disponibilité

Au niveau du contrôle de la disponibilité, les mesures suivantes peuvent être prises pour prévenir la perte ou la destruction accidentelle de données à caractère personnel et garantir un rétablissement rapide de leur disponibilité en cas d'incident physique ou technique :

Exigences
Procédure formalisée de validation de nouvelles procédures informatiques et de modifications importantes d'anciennes procédures
Alimentation électrique sans interruption (ASI)
Installation automatique de détecteurs d'incendie et de fumée
Extincteurs CO2 devant / à l'intérieur du local abritant les serveurs
Sécurisation des bases de données
<ul style="list-style-type: none">• Etablissement d'un concept de sécurisation des bases de données• Conservation de copies de sauvegarde en lieu sûr (externalisation)• Réalisation de copies de sauvegarde à intervalles appropriés selon le principe grand-père-père-fils• Concept de redémarrage pour reconstituer les bases de données• Essais de reconstitution des bases de données
Redondance du matériel informatique, des logiciels et de l'infrastructure

8. Contrôle de l'exécution du mandat

Garantie de l'exécution du mandat conformément aux instructions données : le mandataire doit respecter les instructions reçues, le mandant veillera à ce que ses instructions soient claires et correctement suivies.

Exigences
Contrôle du respect par le mandataire des dispositions applicables en matière de protection des données

Notification de tout non-respect et information si les instructions données pour assurer la sécurité des données semblent insuffisantes
Engagement du personnel du mandataire de respecter les exigences en matière de protection des données
Instructions aux membres du personnel expliquant les données nécessaires à l'exécution du mandat, leur volume et l'utilisation prévue

9. Procédure de contrôles réguliers

Garantie permanente de la conformité aux exigences en matière de protection des données et de sécurité informatique : le mandataire a l'obligation de vérifier régulièrement la conformité aux exigences prévues au contrat et de documenter cette vérification.

<i>Exigences</i>
Mise en place d'un système de gouvernance et de responsabilité en matière de sécurité informatique (adapté aux besoins)
Gestion de la réponse aux incidents
Définition des dispositions applicables au contrôle du processus de modification de procédures
Notification des incidents de sécurité survenus dans le cadre de l'activité de l'entreprise
Contrôle de l'efficacité des mesures prises, à effectuer au moins une fois par an
Paramétrage par défaut des serveurs en veillant à ce qu'il soit sûr et suffisant pour permettre un redémarrage du système en mode sans échec en l'espace de temps prévu

PARTIE A

Annexe 5 : Attestation de mise en œuvre des mesures prévues en matière de sécurité des données

Attestation

de mise en œuvre par le sous-traitant des mesures nécessaires
au respect des exigences en matière de sécurité des données

Le mandataire certifie qu'avant le début du traitement des données, il a mis en œuvre les mesures nécessaires au respect des exigences définies en matière de sécurité des données par le mandant conformément à l'annexe 4 et qu'il a effectué un contrôle pour vérifier cette mise en œuvre.

Partie B

ACCORD DES RESPONSABLES CONJOINTS DU TRAITEMENT

Préambule

L'utilisation de la plateforme de WBG pour les besoins du marketing d'affiliation nécessite une interaction entre WBG, le Publisher et l'Annonceur dans les limites définies ci-dessous (« la **collaboration** ») et entre le Publisher et l'Annonceur au regard de la législation en matière de protection des données conformément à l'article 26 du RGPD (cf. Partie C : ACCORD DES RESPONSABLES CONJOINTS DU TRAITEMENT). A cet effet, les parties se donneront mutuellement accès à des données à caractère personnel ou procéderont à leur collecte et traitement pendant leur collaboration.

Le présent accord est conclu entre l'Annonceur et WBG. A titre complémentaire, l'Annonceur et le Publisher mandaté concluent un autre ACCORD DES RESPONSABLES CONJOINTS DU TRAITEMENT pour l'interaction ayant son importance au regard de la législation en matière de protection des données (Partie D). Cet accord est également conclu pour le cas où des Annonceurs feraient appel à certains Publishers pour l'insertion d'annonces / de publicités.

Dans la présente Partie B, les parties précisent l'étendue de leur collaboration, leurs obligations réciproques, leurs rôles et responsabilités dans le cadre des obligations qui leur incombent en matière de protection des données.

1. Etendue de la collaboration

Dans le cadre de leur collaboration, les responsables du traitement agiront en tant que responsables conjoints. Les rôles des responsables du traitement et les tâches rattachées sont précisés en annexe 1. Si une partie est seule responsable d'une opération de traitement des données, elle assurera sous sa responsabilité le respect de toutes les dispositions applicables en matière de protection des données. Toutefois, de telles procédures de traitement des données ne font pas l'objet du présent Accord.

Le traitement conjoint des données et le type des données à caractère personnel collectées et traitées dans le cadre de la collaboration sont définis en annexe 1.

2. Obligations du responsable du traitement, sous-traitants

2.1 Les responsables traiteront les données à caractère personnel en se conformant aux dispositions applicables en matière de protection des données. Dans leurs rapports avec les tiers, les deux parties et le Publisher sont conjointement responsables du respect des dispositions applicables au traitement conjoint des données. Dans les rapports entre elles, l'étendue de leur responsabilité quant au respect de ces dispositions est définie en annexe 1 qui précise les procédures de traitement des données dont elles ont respectivement la charge.

2.2 Dans le cadre de leur collaboration, les responsables du traitement utiliseront les données à caractère personnel pour les finalités décrites en annexe 1. Chaque responsable du traitement est seul responsable de tout traitement de données allant au-delà de la responsabilité conjointe et doit veiller sous sa propre responsabilité au respect des exigences.

Si les parties traitent des données à caractère personnel objet du contrat à d'autres finalités que celles qui ont été décrites, elles s'informeront mutuellement dans les limites raisonnables dans la mesure où cette information est imposée par la loi.

2.3 Les responsables du traitement veilleront à ce que toutes les personnes intervenant dans le traitement de données à caractère personnel soient tenues ou seront tenues de respecter la confidentialité et ne traiteront les données à caractère personnel que sur instruction du responsable du traitement.

- 2.4 Les données à caractère personnel doivent être exactes et, si nécessaire, tenues à jour. La collecte et le traitement des données à caractère personnel doivent être adéquats, pertinents et limités à ce qui est nécessaire au regard des finalités du transfert et du traitement.
- 2.5 Les responsables du traitement ne feront intervenir un sous-traitant pour le traitement de données à caractère personnel que si un accord conforme aux exigences de la loi a été conclu avec ce sous-traitant. Les responsables du traitement ne transmettront les données à caractère personnel à des tiers que dans la mesure où cette transmission est effectivement nécessaire au respect des obligations résultant de leur collaboration et à condition qu'elle soit pertinente et autorisée par la loi et que les destinataires des données à caractère personnel soient indiquées à l'autre partie.

3. Mesures techniques et organisationnelles

Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, les responsables du traitement mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

- la pseudonymisation et le chiffrement des données à caractère personnel ;
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et de services de traitement ;
- des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans les délais appropriés en cas d'incident physique ou technique ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

4. Responsabilité du respect de la législation en matière de protection des données et des droits des personnes concernées

- 4.1 En règle générale, le responsable du traitement qui a initialement collecté les données à caractère personnel ou directement conclu le contrat avec la personne concernée restera le point de contact central pour les personnes concernées. En règle générale, il s'agit de l'Annonceur qui est en contact direct avec le client et qui a collecté les données en vue de la conclusion du contrat.
- 4.2 Les personnes concernées disposent de différents droits sur les données à caractère personnel traitées par les responsables du traitement. Les responsables du traitement s'engagent à exécuter leurs obligations respectives conformément aux dispositions de la législation applicable en matière de protection des données.
- 4.3 En application des articles 13 et 14 du RGPD, un certain nombre d'informations doivent être fournies aux personnes concernées. Les parties conviennent qu'en ce qui concerne les traitements des données visés en annexe 1 de la Partie C, le Publisher se chargera de la fourniture de ces informations. Par ailleurs, il appartient à l'Annonceur de fournir aux personnes concernées par tout moyen approprié les informations sur les activités de traitement des données visées en annexe 1 de la Partie B conformément à la procédure décrite ci-dessous.
- 4.4 Les responsables du traitement se prêteront mutuellement assistance dans le cadre de l'exécution de leurs obligations contractuelles et/ou légales en se fournissant sur les activités de traitement les informations dont ils ont besoin pour pouvoir se conformer aux exigences. WBG communiquera à l'Annonceur une note explicative de sa politique de protection des données. L'Annonceur transmettra cette note à ses clients finaux pour les renseigner sur le traitement des données effectué par WBG dans le cadre de l'utilisation des Services de marketing d'affiliation. Nonobstant la fourniture de cette note explicative, l'Annonceur demeure responsable du respect de toutes les obligations juridiques lui incombant, notamment ses obligations d'information.
- 4.5 Les personnes concernées ont le droit de demander des informations sur le traitement des données à caractère personnel dans les conditions prévues par la loi. Les personnes concernées par la collaboration peuvent également demander aux responsables du traitement de rectifier ou d'effacer leurs données ou de

limiter l'accès à celles-ci. Dans les cas prévus par la loi, elles peuvent s'opposer à tout moment, pour des raisons tenant à leur situation particulière, à un traitement de leurs données à caractère personnel en s'adressant aux responsables du traitement.

Les parties conviennent que, d'une façon générale, l'Annonceur est responsable de la suite à donner aux demandes des personnes concernées. Il reste le point de contact central pour les personnes concernées.

Les responsables précisent que les personnes concernées par le traitement peuvent exercer auprès de chaque responsable du traitement les droits liés au traitement de leurs données à caractère personnel, ceci sans préjudice de l'article 82 du RGPD.

Les responsables du traitement feront tout ce qui est nécessaire et approprié pour donner suite aux demandes en agissant également au nom de l'autre responsable du traitement et en s'engageant à collaborer à cet effet. En tout état de cause, les responsables du traitement se prêteront mutuellement toute l'assistance pouvant être exigée raisonnablement.

- 4.6 Les obligations de notification prévues par les articles 33 et 34 du RGPD seront exécutées par le responsable du traitement chez lequel l'incident à notifier est survenu. En cas de survenance d'un incident soumis à notification, les parties s'informeront mutuellement sans délai dans la mesure où un traitement objet du présent accord est concerné. L'autre partie fera ses meilleurs efforts pour prêter au responsable du traitement devant notifier l'incident toute l'assistance dont il a besoin pour élucider les faits et prendre les mesures nécessaires à la protection des personnes concernées. Il appartient au responsable du traitement tenu à la notification de statuer sur la nécessité, le contenu et l'étendue des mesures à prendre.
- 4.7 Par ailleurs, si et dans la mesure où des personnes concernées demandent des informations sur le contenu essentiel des dispositions prévues dans la PARTIE B, la fourniture des informations nécessaires relève de la responsabilité de l'Annonceur dès lors qu'elle est imposée par la législation applicable. Si une personne concernée demande ces informations, les responsables du traitement lui communiqueront la présente section de cette PARTIE B après s'être mis d'accord entre eux.
- 4.8 Chaque responsable du traitement tient sous sa propre responsabilité un registre des activités de traitement. Les responsables du traitement se fourniront mutuellement les informations nécessaires à la tenue de ces registres.
- 4.9 Si nécessaire, les responsables du traitement se prêteront mutuellement assistance dans les limites raisonnables pour effectuer une analyse d'impact relative à la protection des données ainsi que dans le cadre de la consultation préalable de l'autorité de contrôle si cela est utile et autorisé par la loi. Chaque responsable du traitement fournira à l'autre responsable du traitement à sa demande les informations et documents nécessaires à cet effet.
- 4.10 Chaque responsable du traitement supportera les frais éventuellement engagés dans le cadre de l'exécution des obligations résultant de la présente PARTIE B. Les clauses du présent Accord s'appliquent sans préjudice des dispositions des CGV (Conditions Générales de Vente) et de tout accord complémentaire relatif à l'utilisation des Services de marketing d'affiliation.

5. Responsabilité

La responsabilité entre les responsables du traitement est régie par la loi.

6. Dispositions applicables en cas de conflit entre les textes

Les dispositions prévues par les CGV pour l'utilisation des Services de marketing d'affiliation sont remplacées par les clauses du présent Accord dans la mesure où celui-ci prévoit des dispositions particulières. Pour le surplus, les dispositions relatives à l'utilisation des Services de marketing d'affiliation s'appliquent à titre subsidiaire.

PARTIE B

ANNEXE 1 : Rôles, tâches et étendue de la collaboration entre l'Annonceur et WBG

WBG met à disposition une plateforme de marketing d'affiliation. Pour les besoins de son utilisation, elle conclut des accords séparés (« CGV ») avec l'Annonceur et le Publisher. Le rôle de WBG consiste à permettre la facturation des ventes générées via la plateforme. L'Publisher déclenche le traitement des données en publiant une annonce publicitaire fournie par l'Annonceur et affectée d'un code de suivi. De cette manière, le client potentiel est dirigé vers la page de renvoi prédéfinie par l'Annonceur.

Sur la base de l'accord contractuel, l'Annonceur transmet à WBG les données nécessaires à la facturation des prestations de le Publisher pour permettre à WBG de respecter ses obligations contractuelles. Par ailleurs, WBG propose à l'Annonceur des Publishers adaptés aux produits / services mis en vente par l'Annonceur. A cet effet, WBG sélectionne dans ses bases de données les Publishers dont on peut supposer qu'eu égard aux exigences de l'Annonceur, ils sont particulièrement adaptés aux activités de marketing de celui-ci. Enfin, WBG établit pour les Publishers un tableau indiquant les produits proposés par l'Annonceur via la plateforme en précisant le volume des produits vendus. De cette manière, le Publisher peut sélectionner les annonces publicitaires les plus intéressantes pour lui.

Dans le cadre de la responsabilité conjointe, les rôles sont répartis comme suit :

Procédure	Finalités / étendue	Rôles et tâches	Traitement des catégories de données / accès aux catégories de données / personnes concernées
Transfert de données par l'Annonceur à WBG afin de permettre la facturation à l'égard de le Publisher / l'Annonceur et la conservation des données nécessaires au respect des obligations de conservation prévues en droit fiscal et commercial	Fourniture de données sur les ventes générées par les Publishers via la plateforme afin de permettre la facturation à l'égard de l'Annonceur / le Publisher et l'exécution des obligations incombant à WBG en application du droit fiscal et commercial	<u>Annonceur</u> : transfert des données à WBG <u>WBG</u> : traitement des données fournies pour les finalités définies	Personnes concernées : les clients de l'Annonceur ayant conclu un contrat avec celui-ci par l'intermédiaire de le Publisher Les données suivantes sont concernées : <ul style="list-style-type: none"> • Coordonnées de l'Annonceur • Coordonnées de l'agence (si elles sont disponibles) • Identifiant de l'Annonceur • Identifiant de l'agence • Identifiant du programme • Données de facturation • Données du contrat • Identifiant de le Publisher
Analyse des données des transactions pour gérer et développer la plateforme et lutter contre les abus et la fraude	Utilisation des données pour détecter les abus / lutter contre la fraude et, sous forme anonymisée, pour : <ul style="list-style-type: none"> • la prévision des capacités • l'optimisation des processus • l'établissement de rapports sur l'utilisation de la plateforme • le développement de la plateforme 	<u>WBG</u> : définition des données à transmettre à WBG pour les finalités indiquées (analyse des données indiquées) <u>Annonceur</u> : transfert de données à WBG	Personnes concernées : les clients de l'Annonceur ayant conclu un contrat avec celui-ci par l'intermédiaire de le Publisher Les données suivantes sont concernées : <ul style="list-style-type: none"> • Identifiant de l'Annonceur • Identifiant de l'Agence • Identifiant de le Publisher • Identifiant du programme • Détails du programme (frais, commission, supercommission) • Données de facturation • Données et état des transactions • Horodatage
Reporting pour le Publisher	Etablissement de rapports pour le Publisher afin de lui permettre de vérifier les ventes et d'optimiser ses propres activités de commercialisation	<u>WBG</u> : définition des données à transmettre à WBG pour ces finalités (établissement de rapports sur la base des données) <u>Annonceur</u> : transfert de données à WBG	Personnes concernées : les clients de l'Annonceur ayant conclu un contrat avec celui-ci par l'intermédiaire de le Publisher Les données suivantes sont concernées : <ul style="list-style-type: none"> • Données de facturation • Code des bons d'achat • Données et état des transactions • Horodatage

			<ul style="list-style-type: none"> • Type de matériel utilisé par l'utilisateur • Navigateur utilisé • Nombre de clics sur l'annonce • URL consultée par l'utilisateur
Recommandation à l'Annonceur des Publishers potentiellement adaptés à ses besoins	Sélection des Publishers susceptibles d'intéresser l'Annonceur sur la base des produits / services vendus par lui ; fourniture à l'Annonceur d'un tableau des Publishers ainsi sélectionnés	<p><u>WBG</u> : sélection des Publishers sur la base des données propres à WBG et fourniture de rapports / propositions à l'Annonceur</p> <p><u>Annonceur</u> : définition avec WBG des critères de sélection des Publishers et fourniture des données</p>	<p>Personnes concernées : le Publisher</p> <p>Les données suivantes sont concernées :</p> <ul style="list-style-type: none"> • Identifiant de le Publisher • Identifiant de la campagne • Produits • Nombre de produits vendus • Date de la vente
Recommandations à le Publisher sur la base des produits potentiellement appropriés	Affichage d'un tableau indiquant à le Publisher les produits proposés par l'Annonceur via la plateforme de WBG. Ce tableau précise également le volume des produits vendus. De cette manière, le Publisher peut sélectionner les produits / moyens publicitaires les plus intéressants pour lui.	<p><u>Annonceur</u> : définition avec WBG des critères de sélection des Publishers et fourniture des données</p> <p><u>Annonceur</u> : concertation avec WBG concernant l'anonymisation des données à des fins de statistiques</p>	<p>Personnes concernées : les clients de l'Annonceur</p> <p>Les données suivantes sont utilisées :</p> <ul style="list-style-type: none"> • Produits • Date de la vente • Nombre de produit achetés

Partie C

ACCORD DES RESPONSABLES CONJOINTS DU TRAITEMENT

entre

l'Annonceur et le Publisher

Préambule

L'utilisation de la plateforme de WBG pour les besoins du marketing d'affiliation nécessite une interaction entre WBG, le Publisher et l'Annonceur et entre le Publisher et l'Annonceur au regard de la législation en matière de protection des données conformément à l'article 26 du RGPD. C'est à l'interaction entre l'Annonceur et le Publisher que s'applique la présente Partie C : ACCORD DES RESPONSABLES CONJOINTS DU TRAITEMENT. Dans le cadre de leur collaboration, l'Annonceur et le Publisher se donneront mutuellement accès à des données à caractère personnel ou procéderont à leur collecte et traitement pendant leur collaboration. Le présent Accord est également conclu pour le cas où des Annonceurs feraient appel à certains Publishers pour l'insertion d'annonces / de publicités.

En **annexe 1** du présent Accord, les parties précisent l'étendue de leur collaboration, leurs obligations réciproques, leurs rôles et responsabilités dans le cadre des obligations qui leur incombent en matière de protection des données.

1. Etendue de la collaboration

Dans le cadre de leur collaboration, les responsables du traitement agiront en tant que responsables conjoints. Les rôles des responsables du traitement et les tâches rattachées sont précisés en annexe 1. Si une partie est seule responsable d'une opération de traitement des données, elle assurera sous sa responsabilité le respect de toutes les dispositions applicables en matière de protection des données. Toutefois, de telles procédures de traitement des données ne font pas l'objet du présent Accord.

Le traitement conjoint des données et le type des données à caractère personnel collectées et traitées dans le cadre de la collaboration sont définis en annexe 1.

2. Obligations du responsable du traitement, sous-traitants

2.1 Les responsables traiteront les données à caractère personnel en se conformant aux dispositions applicables en matière de protection des données. Dans leurs rapports avec les tiers, les deux parties et le Publisher sont conjointement responsables du respect des dispositions applicables au traitement conjoint des données. Dans les rapports entre elles, l'étendue de leur responsabilité quant au respect de ces dispositions est définie en annexe 1 qui précise les procédures de traitement des données dont elles ont respectivement la charge.

2.2 Dans le cadre de leur collaboration, les responsables du traitement utiliseront les données à caractère personnel pour les finalités décrites en annexe 1. Chaque responsable du traitement est seul responsable de tout traitement de données allant au-delà de la responsabilité conjointe et doit veiller sous sa propre responsabilité au respect des exigences.

Si les parties traitent des données à caractère personnel objet du contrat à d'autres finalités que celles qui ont été décrites, elles s'informeront mutuellement dans les limites raisonnables dans la mesure où cette information est imposée par la loi.

2.3 Les responsables du traitement veilleront à ce que toutes les personnes intervenant dans le traitement de données à caractère personnel soient tenues ou seront tenues de respecter la confidentialité et ne traiteront les données à caractère personnel que sur instruction du responsable du traitement.

- 2.4 Les données à caractère personnel doivent être exactes et, si nécessaire, tenues à jour. La collecte et le traitement des données à caractère personnel doivent être adéquats, pertinents et limités à ce qui est nécessaire au regard des finalités du transfert et du traitement.
- 2.5 Les responsables du traitement ne feront intervenir un sous-traitant pour le traitement de données à caractère personnel que si un accord conforme aux exigences de la loi a été conclu avec ce sous-traitant. Les responsables du traitement ne transmettront les données à caractère personnel à des tiers que dans la mesure où cette transmission est effectivement nécessaire au respect des obligations résultant de leur collaboration et à condition qu'elle soit pertinente et autorisée par la loi et que les destinataires des données à caractère personnel soient indiquées à l'autre partie.

3. Mesures techniques et organisationnelles

Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, les responsables du traitement mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

- la pseudonymisation et le chiffrement des données à caractère personnel ;
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et de services de traitement ;
- des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans les délais appropriés en cas d'incident physique ou technique ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

4. Responsabilité du respect de la législation en matière de protection des données et des droits des personnes concernées

- 4.1 En règle générale, le responsable du traitement qui a initialement collecté les données à caractère personnel ou directement conclu le contrat avec la personne concernée restera le point de contact central pour les personnes concernées. En règle générale, il s'agit de l'Annonceur qui est en contact direct avec le client et qui a collecté les données en vue de la conclusion du contrat.
- 4.2 Les personnes concernées disposent de différents droits sur les données à caractère personnel traitées par les responsables du traitement. Les responsables du traitement s'engagent à exécuter leurs obligations respectives conformément aux dispositions de la législation applicable en matière de protection des données.
- 4.3 En application des articles 13 et 14 du RGPD, un certain nombre d'informations doivent être fournies aux personnes concernées. Les parties conviennent qu'en ce qui concerne les traitements des données visés en annexe 1 de la Partie C, le Publisher se chargera de la fourniture de ces informations. Par ailleurs, il appartient à l'Annonceur de fournir aux personnes concernées par tout moyen approprié les informations sur les activités de traitement des données visées en annexe 1 de la Partie B conformément à la procédure décrite ci-dessous.
- 4.4 Les responsables du traitement se prêteront mutuellement assistance dans le cadre de l'exécution de leurs obligations contractuelles et/ou légales en se fournissant sur les activités de traitement les informations dont ils ont besoin pour pouvoir se conformer aux exigences. WBG communiquera à l'Annonceur une note explicative de sa politique de protection des données. L'Annonceur transmettra cette note à ses clients finaux pour les renseigner sur le traitement des données effectué par WBG dans le cadre de l'utilisation des Services de marketing d'affiliation. Nonobstant la fourniture de cette note explicative, l'Annonceur demeure responsable du respect de toutes les obligations juridiques lui incombant, notamment ses obligations d'information.
- 4.5 Les personnes concernées ont le droit de demander des informations sur le traitement des données à caractère personnel dans les conditions prévues par la loi. Les personnes concernées par la collaboration peuvent également demander aux responsables du traitement de rectifier ou d'effacer leurs données ou de

limiter l'accès à celles-ci. Dans les cas prévus par la loi, elles peuvent s'opposer à tout moment, pour des raisons tenant à leur situation particulière, à un traitement de leurs données à caractère personnel en s'adressant aux responsables du traitement.

Les parties conviennent que, d'une façon générale, l'Annonceur est responsable de la suite à donner aux demandes des personnes concernées. Il reste le point de contact central pour les personnes concernées.

Les responsables précisent que les personnes concernées par le traitement peuvent exercer auprès de chaque responsable du traitement les droits liés au traitement de leurs données à caractère personnel, ceci sans préjudice de l'article 82 du RGPD.

Les responsables du traitement feront tout ce qui est nécessaire et approprié pour donner suite aux demandes en agissant également au nom de l'autre responsable du traitement et en s'engageant à collaborer à cet effet. En tout état de cause, les responsables du traitement se prêteront mutuellement toute l'assistance pouvant être exigée raisonnablement.

- 4.6 Les obligations de notification prévues par les articles 33 et 34 du RGPD seront exécutées par le responsable du traitement chez lequel l'incident à notifier est survenu. En cas de survenance d'un incident soumis à notification, les parties s'informeront mutuellement sans délai dans la mesure où un traitement objet du présent accord est concerné. L'autre partie fera ses meilleurs efforts pour prêter au responsable du traitement devant notifier l'incident toute l'assistance dont il a besoin pour élucider les faits et prendre les mesures nécessaires à la protection des personnes concernées. Il appartient au responsable du traitement tenu à la notification de statuer sur la nécessité, le contenu et l'étendue des mesures à prendre.
- 4.7 Par ailleurs, si et dans la mesure où des personnes concernées demandent des informations sur le contenu essentiel des dispositions prévues dans la PARTIE B, la fourniture des informations nécessaires relève de la responsabilité de l'Annonceur dès lors qu'elle est imposée par la législation applicable. Si une personne concernée demande ces informations, les responsables du traitement lui communiqueront la présente section de cette PARTIE B après s'être mis d'accord entre eux.
- 4.8 Chaque responsable du traitement tient sous sa propre responsabilité un registre des activités de traitement. Les responsables du traitement se fourniront mutuellement les informations nécessaires à la tenue de ces registres.
- 4.9 Si nécessaire, les responsables du traitement se prêteront mutuellement assistance dans les limites raisonnables pour effectuer une analyse d'impact relative à la protection des données ainsi que dans le cadre de la consultation préalable de l'autorité de contrôle si cela est utile et autorisé par la loi. Chaque responsable du traitement fournira à l'autre responsable du traitement à sa demande les informations et documents nécessaires à cet effet.
- 4.10 Chaque responsable du traitement supportera les frais éventuellement engagés dans le cadre de l'exécution des obligations résultant du présent Accord. Les clauses de celui-ci s'appliquent sans préjudice des dispositions des CGV et de toute accord complémentaire relatif à l'utilisation des Services de marketing d'affiliation, tels qu'ils ont été conclus entre la société Webgains France SARL et la partie concernée.

5. Responsabilité

La responsabilité entre les responsables du traitement est régie par la loi.

6. Dispositions applicables en cas de conflit entre les textes

Les dispositions prévues par les CGV pour l'utilisation des Services de marketing d'affiliation de WBG sont remplacées par les clauses du présent Accord dans la mesure où celui-ci prévoit des dispositions particulières. Pour le surplus, les dispositions relatives à l'utilisation des Services de marketing d'affiliation s'appliquent à titre subsidiaire.

PARTIE D

ANNEXE 1: Rôles, tâches et étendue de la collaboration entre l'Annonceur et le Publisher si ce dernier est chargé de l'intermédiation par l'Annonceur

WBG met à disposition une plateforme de marketing d'affiliation. Pour les besoins de son utilisation, elle conclut des accords séparés (« CGV ») avec l'Annonceur et le Publisher. Le rôle de WBG consiste à permettre la facturation des ventes générées via la plateforme. Le Publisher déclenche le traitement des données en publiant une annonce publicitaire fournie par l'Annonceur via la plateforme et affectée d'un code de suivi. De cette manière, le client potentiel est dirigé vers la page de renvoi prédéfinie par l'Annonceur.

Sur la base d'un accord contractuel séparé, l'Annonceur transmet à WBG les données nécessaires à la facturation des prestations de le Publisher pour permettre à WBG de respecter ses obligations contractuelles. Par ailleurs, WBG propose à l'Annonceur des Publishers adaptés aux produits / services mis en vente par l'Annonceur. A cet effet, WBG sélectionne dans ses bases de données les Publishers dont on peut supposer qu'eu égard aux exigences de l'Annonceur, ils sont particulièrement adaptés aux activités de marketing de celui-ci.

Dans le cadre de la responsabilité conjointe, les rôles sont répartis comme suit entre l'Annonceur et le Publisher :

Procédure	Finalités / étendue	Rôles et tâches	Traitement des catégories de données / accès aux catégories de données / personnes concernées
Redirection de l'utilisateur par le Publisher vers la page à laquelle renvoie l'annonce publicitaire de l'Annonceur si on clique sur celle-ci	Le Publisher utilise l'annonce publicitaire de l'Annonceur affectée d'un code de suivi à des fins publicitaires (« affichage »). Après avoir cliqué sur l'annonce, l'utilisateur est redirigé vers la page de renvoi prédéfinie.	<u>Publisher</u> : intégration de la publicité pixelisée dans le cadre de ses propres opérations de marketing et renvoi de la demande après un clic sur la publicité pour la consultation de la page de renvoi prédéfinie par l'Annonceur <u>Annonceur</u> : mise à disposition de la publicité et du script	Personne Concernée : client potentiel de l'Annonceur. Les données suivantes sont concernées : <ul style="list-style-type: none">• Adresse IP• Référent• Type de navigateur• Date et heure de la consultation (horodatage)• Identifiant du programme• Identifiant de le Publisher• Identifiant de l'étude probabiliste• Identifiant de l'événement• Valeur• Identifiant de la référence
