CONDITIONS GÉNÉRALES DE TRAITEMENT DE DONNEES A CARACTERE PERSONNEL

PREAMBULE

La Société KETIL MEDIA, RC Nanterre 790 128 581, dont le siège social est au 76 boulevard de la République, représentée par Vincent Buffin en sa qualité de Président

Ci-après dénommée la « régie publicitaire »,

commercialise les espaces publicitaires de différents media auprès d'annonceurs et d'agence media, dénommés conjointement ci-après « les Clients » et dans ce cadre utilise en mode SAAS des logiciels - notamment Sales Force - qui peuvent collecter des données nécessaires pour le suivi de son activité commerciale.

Les présentes conditions générales, définissent les conditions des traitements de données à caractère personnel que la Régie Publicitaire devra mettre en œuvre pour le compte du Client dans la cadre de la réglementation RGDP qui entre en vigueur le 25 mai 2018. Elles sont, de fait, annexées aux conditions générales de ventes qui lient les Clients et la Régie Publicitaire.

1. DÉFINITIONS

Pour les besoins du présent article, les termes suivants «données à caractère personnel», «délégué à la protection des données», «traiter/traitement», «responsable du traitement», «destinataire», «sous-traitant» et «transférer/transfert» ont la même signification que celle qui leur est donnée dans le Règlement Européen 2016/679 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 (le «RGPD»).

2. OBLIGATIONS DE LA RÉGIE PUBLICITAIRE

2.1. Respect des instructions du Client et de la réglementation

La Régie Publicitaire s'engage à :

(i) Traiter les données à caractère personnel collectées uniquement dans le cadre de son activité professionnelle.

(ii) Respecter la réglementation applicable aux données à caractère personnel traitées ;

(iii) Veiller à ce que les personnes autorisées à accéder aux données à caractère personnel en vertu du présent Contrat reçoivent la formation nécessaire en matière de protection des données à caractère personnel ;

(iv) Communiquer le nom et les coordonnées du DPO désigné par la Régie Publicitaire à tout client en faisant la demande ;

(v) Ne pas concéder, louer, céder ou autrement communiquer à une autre personne, tout ou partie des données à caractère personnel, même à titre gratuit, ainsi que ne pas utiliser les données à caractère personnel à d'autres fins que celles prévues prévue pour son activité de régie publicitaire ;

(vi) Prendre en compte, s'agissant de ses outils, produits, applications ou Services SaaS, les principes de protection des données dès leur conception.

2.2. Sécurité, confidentialité, violation et destruction des données

La Régie Publicitaire s'engage à :

(i) Prendre toutes précautions utiles afin de préserver la confidentialité et la sécurité des données à caractère personnel, et notamment, empêcher qu'elles ne soient déformées, endommagées ou communiquées à tout tiers non autorisé, et plus généralement, à mettre en œuvre les mesures techniques et d'organisation appropriées telles que détaillées à l'article « Sécurité des données à caractère personnel » de l'Annexe 1 pour protéger les données à caractère personnel contre la destruction accidentelle illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment, lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que, contre toute forme de traitement illicite, étant précisé que ces mesures doivent assurer, compte tenu de l'état de l'art, un niveau de sécurité approprié au regard des risques présentés par les traitements et la nature des données à protéger ;

(ii) Mettre en place des habilitations pour restreindre l'accès des personnes aux données à caractère personnel et ne communiquer les données à caractère personnel qu'aux personnes ayant besoin d'en connaître, en veillant à ce que ces personnes soient soumises à une obligation contractuelle ou légale de confidentialité et de sécurité appropriée ;

(iii) Mettre à jour les mesures de sécurité compte tenu de l'évolution de la technique, sans qu'il ne puisse résulter une diminution du niveau de sécurité ;

(iv) Notifier aux clients toute violation de données à caractère personnel, accompagnée de toute documentation utile dans les meilleurs délais et au plus tard huit (8) heures après en avoir pris connaissance, notamment afin de se conformer à l'obligation de notifier à la CNIL toute violation de données dans les conditions visées à l'article 33 du RGPD ;

(v) Mettre en place les mesures nécessaires à la protection des données à caractère personnel en cas de violation des données, en consultation avec ses clients et ses agences media pour limiter tout effet négatif sur les personnes affectées par la violation ;

(vi) Respecter les durées de conservation des données à caractère personnel, telles que spécifiées en Annexe 1 ;

2.3. Assistance

La Régie Publicitaire s'engage à :

(i) Aider et collaborer avec ses Clients afin de garantir le respect des obligations incombant à ce dernier, conformément à la réglementation applicable en matière de protection des données à caractère personnel ;

(ii) Fournir aux personnes concernées l'information relative aux traitements de collecte de données à caractère personnel. La formulation et le format de l'information doivent être convenus avec le Client préalablement à tout traitement de collecte de données.

(iii) Répondre dans les meilleurs délais à toute demande du Client portant sur les données à caractère personnel traitées, afin de permettre au Client de prendre en compte, dans les délais impartis, les éventuelles requêtes des intéressés (droit d'accès, droit de rectification, droit à l'effacement, etc.), et de manière plus générale tenir compte de la nature du traitement et aider le Client par des mesures techniques et organisationnelles appropriées à s'acquitter

de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits;

(iv) Lorsque les personnes concernées exercent auprès de la Régie Publicitaire des demandes d'exercice de leurs droits, adresser ces demandes dès leur réception par courrier électronique aux adresses email qui devront être communiquées par le Client à la . Le Client assurera, à défaut d'instruction écrite contraire de sa part, le traitement de ces demandes ;

(v) Fournir au Client toute information et toute assistance nécessaire pour permettre à ce dernier de respecter ses obligations en cas de violation de données à caractère personnel (incluant au minimum la nature de la violation, les catégories et le nombre approximatif de personnes concernées et de données à caractère personnel touchées par la violation, ainsi que les conséquences probables de la violation) ;

2.4. Sous-traitance ultérieure

La Régie Publicitaire s'engage à ne pas sous-traiter l'exécution les traitements sans l'accord préalable, écrit et spécifique du Client.

La Régie Publicitaire demeure en tout état de cause pleinement responsable de l'exécution, par tout sous-traitant de second rang (préalablement agréé par le Client), des obligations lui incombant et s'engage :

(i) À répercuter auprès de ses sous-traitants les engagent et obligations auxquels il est tenu au titre du Contrat ;

(ii) À communiquer au Client, sur demande de celui-ci, les termes des contrats conclus avec ses sous-traitants de second rang ;

2.5. Transferts de données à caractère personnel hors-UE

La Régie Publicitaire s'engage, que ce soit à raison des Prestations qu'il réalise ou à raison des Prestations réalisées dans le cadre d'un recours à la sous-traitance autorisée selon les conditions du Contrat, à ne pas transférer les données à caractère personnel traitées dans le cadre du Contrat, hors de l'Union Européenne ou des pays dits de « protection adéquate » sans l'autorisation préalable et écrite du Client, ce dernier devant en effet pouvoir procéder, préalablement au transfert :

(i) À la mise en place de garanties appropriées telles que prévues par la réglementation applicable en matière de protection des données à caractère personnel (BCR sous-traitants, clauses types de protection des données adoptées par la Commission responsable du traitement/sous-traitant, adhésion de l'importateur au UE-US Privacy Shield arrangement, code de conduite ou mécanisme de certification approuvés),

(ii) À la réalisation des formalités et à l'obtention le cas échéant de l'autorisation préalable de transférer les données personnelles sur la base d'un engagement de l'importateur des données personnelles recueilli dans le cadre d'un mécanisme alternatif de protection des données à caractère personnel accepté par la CNIL et,

(iii) À l'information des personnes concernées.

Néanmoins, si la Régie Publicitaire est tenu de procéder à de tels transferts en vertu du droit applicable, celle-ci s'engage à informer immédiatement le Client, sauf impossibilité légale. Les engagements souscrits par la Régie Publicitaire au titre du présent article, ne peuvent être soumis à aucune limitation de responsabilité de la Régie Publicitaire.

2.6. Audit

Sur première demande du Client et dans un délai raisonnable, la Régie Publicitaire s'engage à mettre à disposition du Client toutes les informations nécessaires pour démontrer le respect de ses obligations telles qu'énoncées dans ce Contrat et lui incombant en tant que sous-traitant et à permettre la réalisation d'audit(s), y compris des inspections par le Client ou un autre auditeur que le Client aura mandaté et contribuer à ces audits.

Le Client pourra particulièrement contrôler l'adéquation des mesures techniques et organisationnelles prises par la Régie Publicitaire, notamment en se rendant dans ses locaux, ce que la Régie Publicitaire reconnaît et accepte expressément.

3. CONFIDENTIALITÉ

Chaque Partie s'engage à limiter les demandes d'informations auprès de l'autre Partie, notamment les Informations Confidentielles, à celles strictement nécessaires à la bonne exécution du Contrat.

Par Information Confidentielle, on entend notamment (cette liste n'étant pas exhaustive) :

- toute information relative à une Partie, communiquée par elle (la « Partie Communicante »), à l'autre Partie (la « Partie Réceptrice »), de nature stratégique, technique, commerciale, financière, juridique ou autre, communiquée sous quelque forme que ce soit, par oral ou par écrit, courrier électronique, télécopie, dessins, logiciels, code source, copie électronique de documents, spécifications, information, graphiques, enregistrements, reproduction graphique ou information digitale communiquée à la Partie Réceptrice avant ou après la signature ou la date de l'accord et qui a trait à la Partie Communicante et/ou à ses produits ;
- Les traitements eux-mêmes, l'identité des personnes qui sont impliquées sur ces derniers, qu'elles travaillent pour une des Parties ou dans l'équipe de leurs conseillers ainsi que l'existence, le contenu, la nature, l'étape de réalisation et l'évolution des traitements ;
- L'identité de toute autre société impliquée, ou que les Parties envisagent d'impliquer dans les traitements ; et
- Toute donnée à caractère personnel objet d'un traitement en application du présent Contrat ;
- Le présent Contrat et tout ce qui s'y rapporte ;
- Les Parties conviennent que toute information ci-dessus décrite et divulguée par la Partie Communicante n'aura pas à être marquée par elle comme « confidentielle » pour (i) être considérée comme une Information Confidentielle et (ii) être protégée en tant que telle en vertu du présent accord.

N'est pas considérée comme une Information Confidentielle, toute information qui :

- Serait dans le domaine public au moment de sa transmission, ou y tomberait postérieurement, indépendamment de toute violation d'une clause du Contrat, où ; Serait connue par la Partie à laquelle elle était destinée avant qu'elle ne lui soit transmise par l'autre Partie, sous réserve que la Partie destinataire de l'Information puisse justifier de façon valable en avoir eu connaissance préalablement, où ;
- Aurait été communiquée par un tiers de manière licite et reçue de bonne foi, ou ;
- Aurait été communiquée suite à une demande administrative ou judiciaire ou ;

- Constituerait une information dont l'utilisation ou la divulgation a été spécifiquement autorisée par écrit par l'autre Partie.

La Partie Réceptrice s'engage à n'utiliser l'Information Confidentielle de la Partie Communicante qu'en vue de l'exécution de ses obligations établies dans le Contrat.

Ainsi, chaque Partie ne peut divulguer l'Information Confidentielle de l'autre Partie qu'à ceux de ses employés, mandataires sociaux, membres du groupe auquel il appartient ou cocontractants qui ont à en connaître à cet effet, et s'engage à ne pas communiquer, reproduire, publier ou divulguer de quelque façon que ce soit cette Information Confidentielle à des tiers, à moins que l'autre Partie n'ait donné son consentement préalable et écrit.

L'Information Confidentielle ne peut être autrement divulguée que dans la seule mesure requise par la loi, y compris par toute autorité de réglementation ou de contrôle. Toutefois, dans ces circonstances et pour autant que la loi l'y autorise, la Partie Réceptrice obligée de divulguer l'Information Confidentielle de la Partie Communicante devra en avertir cette dernière promptement et par écrit, de façon à lui permettre de chercher toute mesure de protection qu'elle jugerait nécessaire.

Chaque Partie s'engage à prendre toutes mesures de sécurité, notamment matérielle, pour assurer la conservation et l'intégrité des Informations Confidentielles traités pendant la durée du présent Contrat.

Chaque Partie se porte fort du respect de l'obligation de confidentialité prévue au présent article par ses employés, mandataires sociaux, cocontractants et entités de leur groupe le cas échéant, et fera en sorte que ces derniers soient liés par une obligation de confidentialité aussi stricte.

Chaque Partie s'engage expressément à n'utiliser les Informations Confidentielles de l'autre Partie, dont elle aurait connaissance, que dans le cadre du Contrat et à n'effectuer aucune duplication, de quelque nature que ce soit, des Informations Confidentielles transmises, si de telles duplications n'ont pas été prévues dans le cadre du présent Contrat.

Chaque Partie restituera à l'autre Partie, dans les huit (8) Jours suivant la date de fin du Contrat, l'Information Confidentielle de cette autre Partie (y compris toute reproduction totale ou partielle) ou, dans la mesure où une telle restitution ne peut être effectuée, lui transmettra une attestation de destruction.

Les obligations issues du présent article resteront en vigueur pendant une durée de deux (2) années suivant l'expiration et/ou la résiliation du Contrat et du Contrat de Référence, pour toute raison.

4. GARANTIES ET ASSURANCE

4.1. Garanties

Chaque Partie garantit à l'autre :

- Qu’elle est pleinement habilitée à conclure le Contrat et à remplir les obligations qui lui incombent en vertu des présentes, et qu'aucun engagement contracté par elle précédemment ou à l'avenir n'est de nature à compromettre ou contrarier l'exécution du Contrat, et
- Qu’elle respectera, dans le cadre de l'exécution de ses obligations du Contrat, toutes les lois, codes, et règlements applicables notamment en matière de données à caractère personnel.

La Régie Publicitaire garantit également qu'il indemnisera le Client de tous dommages, pertes, coûts (y compris les frais raisonnables d'avocat et les frais de justice) et dépenses engagées par Client en conséquence :

- Du non-respect de l'une de ses obligations par la Régie Publicitaire au titre du présent Contrat, en ce inclus tout non-respect de la réglementation applicable en matière de données à caractère personnel ; et
- De toute condamnation prononcée à l'encontre du Client dans le cadre de tout recours entraîné par le non-respect de la Régie Publicitaire de toute obligation relevant de sa qualité de (i) sous-traitant, (ii) de responsable de traitement, telles que prévues au présent Contrat.

4.2. Assurance

La Régie Publicitaire s'engage, à ses seuls frais, à souscrire et à maintenir en vigueur, auprès d'une compagnie notoirement solvable, une police d'assurance de responsabilité civile professionnelle et de perte d'exploitation, garantissant les conséquences de la responsabilité qu'elle est susceptible d'encourir dans le cadre de l'exécution du Contrat, en raison des dommages matériels ou immatériels pouvant être causés au Client ou à tout tiers, et/ou à leurs préposés.

En tout état de cause, la Régie Publicitaire veillera à ce que sa couverture soit toujours suffisante au regard des risques inhérents ou consécutifs auxdites exécutions et elle s'engage à aviser immédiatement et par tout moyen le Client de toute réduction des garanties ainsi que de la résiliation éventuelle des contrats d'assurance avec confirmation écrite le jour même.

Le fait de disposer d'une assurance telle que décrite ci-dessus ne dégage en rien la Régie Publicitaire de ses responsabilités, notamment en ce qui concerne les dommages qui ne seraient pas couverts par son assurance ou les dommages dont les montants excéderaient les capitaux garantis par celle-ci.

ANNEXE 1 : TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL

1. Description des traitements faisant l'objet de la Sous-traitance

La Régie Publicitaire est autorisée à traiter les données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) :

Pour les besoins de la présente Annexe 1, les Traitements 1, 2 et 3 pourront être nommés collectivement les « Traitements ».

1.1. Traitement 1 : création d'ordres d'insertion (progiciel AdResa, Mediapilot)

La nature des opérations réalisées par la Régie Publicitaire sur les données est : progiciel de création d'ordres d'insertion.

La ou les finalité(s) du traitement sont : facturation pour vente d'espace publicitaire.

Les données à caractère personnel traitées sont :

- Contact du salarié du Client, chargé de la vente d'espace publicitaire (nom, prénom, email, téléphone, commentaires) ;

La base légale du Traitement 1 est : traitement nécessaire à l'exécution d'un contrat.

1.2. Traitement 2 : création de comptes acheteurs (progiciel Adresa et Mediapilot et Sales Force)

La nature et la finalité des opérations réalisées par la Régie Publicitaire sur les données est : Création de nouveaux comptes acheteur d'espace publicitaire

Les données à caractère personnel traitées sont :

- Contact de l'acheteur d'espace publicitaire (nom, prénom, fonctions, email, téléphone, commentaires) ;

La base légale du Traitement 2 est : intérêt légitime de la Régie Publicitaire

1.3. Traitement 3 : base de données clients (progiciel Sales Force)

La nature des opérations réalisées par la Régie Publicitaire sur les données est : progiciel permettant la constitution par le Client de sa propre base de données de clients, en ce inclus les comptes rendus d'entretien avec lesdits Clients.

La ou les finalité(s) du traitement sont : Constitution d'une base de données acheteurs d'espace publicitaire, incluant des comptes rendus d'entretien.

Les données à caractère personnel traitées sont :

- Contact du salarié du Client (nom, prénom, email, téléphone, commentaires) ;
- Comptes rendus des actions commerciales entre l'acheteur et le vendeur ;

La base légale du Traitement 3 est : intérêt légitime de la Régie Publicitaire.

2. Catégorie de personnes concernées

La catégorie de personnes concernées par les Traitements (1, 2 et 3) est :

- Acheteurs d'espace publicitaire (clients, indépendants et mandataires, incluant les salariés d'agences média, digitale, ou de communication).

3. Sécurité des données à caractère personnel

Afin de garantir un niveau de sécurité adapté aux risques des Traitements, la Régie Publicitaire s'engage à mettre en place les mesures techniques et organisationnelles figurant en annexe 3.

4. Durée de conservation des données à caractère personnel

Les données à caractère personnel récoltées dans le cadre des Traitements 1, 2 et 3 seront conservées par la Régie Publicitaire pour la durée légale.

ANNEXE 2 : SUJETS ET CATÉGORIES DE DONNÉES

Sujets de données : Les données personnelles traitées concernent les catégories d'acteurs suivantes :

- Les clients du Data Supervisor ou contrôleur de données en qualité de propriétaire de sa base de données
- Perspectives du contrôleur de données
- Les visiteurs du site Web du contrôleur des données,
- Les employés du contrôleur des données,

Catégories de données : Les données personnelles traitées concernent les catégories de données suivantes :

- Adresses e-mail,
- Numéro de portable,
- Numéro de téléphone fixe,
- Nom, prénom,
- Fonction et titre
- Adresse postale,
- Ouverture des e-mails reçus,
- Cliquer sur les liens contenus dans les e-mails reçus,
- Les commentaires sur les contacts ajoutés le cas échéant par la Régie Publicitaire

ANNEXE 3 : ANNEXE SUR LA SÉCURITÉ

1. Confidentialité (article 32, paragraphe 1, lit. b, GDPR)

Contrôle d'accès physique

Aucun accès physique non autorisé aux systèmes de traitement de données. Contrôles physiques d'accès selon ISO 27001: 2013 A.11.1-6, notamment les systèmes de contrôle d'accès électronique, l'authentification multifactorielle pour les zones de traitement protégées, les systèmes de détection d'intrusion, les procédures de vidéosurveillance et de gestion des visiteurs.

Contrôle d'accès au système

Pas d'accès non autorisé aux systèmes d'information. Commandes d'accès au système selon la norme ISO 27001: 2013, règles A.11.2.8-9, A.9.1.1-2, A.9.2.1-6, A.9.3.1, A.9.4.1-5, A.13.1.13 et 150 27018: 2014 A.10.8-10, en particulier les mots de passe sécurisés, les mécanismes de verrouillage automatique, l'authentification multifactorielle pour les administrateurs et le cryptage des appareils.

Contrôle d'accès aux données

Aucune opération de lecture, copie, modification ou suppression non autorisée dans les systèmes d'information Contrôle de l'accès aux données selon ISO 27001: 2013 A.9.1.1-2, A.9.2.1-6, A. 9.3.1, A.9.4.1-5, A.12.14 et ISO 27018: 2014 A.10.8-10, en particulier la politique de contrôle d'accès et l'enregistrement d'accès.

Mise en œuvre du contrôle de séparation

Séparer le traitement des données collectées à des fins différentes. Contrôle de séparation selon ISO 27001: 2013 A.9.4.1, isolement / séparation particulièrement logique des locataires.

2. Intégrité (article 32, paragraphe 1, lettre b, GDPR)

Mise en œuvre du contrôle de transfert

Aucune lecture, copie, modification ou annulation non autorisée pendant la transmission ou le transport électronique. Contrôle du transfert selon ISO 27001: 2013 A.13.1.1-3, A.13.2.1-4, A.10.1.1-2, ISO 27018: 2014 A.13.2.1, A.10.1, A .10.6 et A.10.1.1, en particulier la cryptographie sur les réseaux qui transmettent des données en utilisant les normes et les algorithmes de meilleures pratiques de l'industrie tels que TLS ou SSH.

Mise en œuvre du contrôle d'entrée

Déterminer si des données personnelles ont été entrées, modifiées ou supprimées des systèmes d'information. Contrôle d'entrée selon les normes ISO 27001: 2013 A.12.4.1-4 et ISO 27018: 2014 A.12.4.1-2, avec une référence particulière à l'accès aux systèmes.

3. Disponibilité et résilience (article 32, paragraphe 1, lettre b, GDPR)

Vérification de la disponibilité

Protection contre les pertes ou destructions accidentelles ou intentionnelles. Vérifier la disponibilité selon ISO 27001: 2013 A.11.2.1-4, A.12.1.1-2, A.12.2.1, A.12.3.1, A.12.4.1-4, A.12.5. 1, A.12.6.1-2, A.12.7.1, A.13.1.1-3, A.17.1.1-3, A.17.2.1, en particulier les concepts de sauvegarde, redondance, continuité de service et récupération après sinistre, procédures

opérationnelles, protection contre les logiciels malveillants, pare-feu et gestion de la sécurité réseau, gestion des vulnérabilités.

Capacité de récupération (article 32, paragraphe 1, lit. c, GDPR)

Capacité de récupérer dans un délai approprié après un événement de perturbation. Capacité de récupération selon ISO 27001: 2013 A.12.3.1, A.17.1.1-3 et A.17.2.1, en particulier les concepts de sauvegarde, de redondance, de continuité opérationnelle et de reprise après sinistre.

4. Processus d'évaluation périodique de l'efficacité des mesures (article 32, paragraphe 1, alinéa d, du RGPD, article 25, section 1, du RGPD)

Gestion de la protection des données

Approche systématique de la gestion de la protection des données. Exploitation d'un système de gestion de la sécurité de l'information et de la protection des données selon ISO 27001, ISO 27002 et ISO 27018.

Gestion des réponses aux incidents

Approche systématique de la gestion des incidents. Gestion de la réponse aux accidents selon ISO 27001: 2013 A.16.1.1-7, ISO 27018: 2014 A.16.1 et A.9.1, en tenant compte des obligations de notification légales et contractuelles applicables.